Building a 2-Tier, Offline-Root, Internal PKI with an IIS CDP on MS Windows Server 2012 R2

Windows Server 2012 R2

Abstract:

(jump to TOC)

This document provides a soup to nuts demonstration of how to build a 2-tier, offline-root, internal PKI with an IIS CDP on MS Windows Server 2012 R2. The procedure is the same for Windows Server 2016, and Windows Server 2019.

Document Revision and History:

(jump to TOC)

version	date	description
1.0	4/15/2015	• initial publication for presentation at LRITA (www.LRITA.org)
1.1	4/17/2015	• added verbiage in 'Warnings' section • fixed an error regarding renewal in the sub/policy/issuing CA's CAPolicy.inf
1.2	4/29/2015	• added eBook information to bibliography • cleaned up TOC links • corrected screenshots of DC's local certificate store after creation of sub/policy/issuing CA • tightened verbiage on all screenshots of DC's local certificate store
1.3	4/29/2015	• added the 'Special Thanks' section
1.4	8/13/2015	• fixed a typo
1.5	8/20/2015	• updated the 'Buying from Amazon', 'Digital Signing', and certificate chaining diagrams • cleaned up language and misconceptions around chaining (the diagram and the terminology section)
1.6	8/27/2015	• cleaned up errors in CA extensions codes is CertUtil.exe files • clarified chaining diagram
1.7	8/28/2015	• clarified verbiage in CAPolicy and CertUtil files • added a step to publish CRL after root issues certificate to sub/policy/issuing CA
1.8	9/2/2015	• minor typographical edits to certificate chaining diagram • clarified verbiage in CAPolicy and CertUtil files • added deltaOverlap info into CertUtil files • added to the 'Terminology' section • added KRA explanation
1.9	9/15/2015	• clarified verbiage in 'algorithms' section • added caveat in root CA's certutil.exe file for not needing to specify Forest's configuration partition because root CA is offline • added suggestion for a 15 or fewer character name for CAs

		• added a warning that the CAPolicy.inf and Certutil.exe files have been changed since initial publication, so screenshots might not always reflect the values from those files • added to the 'Terminology' section • clarified CAPolicy and CertUtil files
1.10	10/5/2015	• added a note in the CertUtil.exe files about '%1_' in the AIA extensions
1.11	10/5/2015	• clarified the verbiage of 'issue' in the 'terminology' section • clarified the verbiage of 'renewal' in the 'terminology section • cleaned up 'private/public' nomenclature in 'Amazon' diagram • cleaned up 'configured from' verbiage in 'Certificate Chaining' diagram
1.12	10/9/2015	• added 'OID' to the 'Terminology' section
1.13	10/22/2015	• added 'Appendix A'
1.14	10/22/2015	• added 'Appendix B'
1.15	11/17/2015	• updated 'Algorithms' section, and 'Terminology' section
1.16	1/22/2016	• updated NTAuthCertificates info on ADSIEdit explanation
1.17	2/8/2016	• clarified and fix errors in the info on ADSIEdit explanation • added info on when to publish the root CA's certificate to AD • cleaned up typos in the 'Terminology' section • added info on LoadDefaultTemplates to the CAPolicy.inf files • added info about preventing the sub/policy/issuing CA from issuing certificates until it's fully configured
1.18	4/18/2016	• added info to Bibliography • added info into sub/policy/issuing CA's CAPolicy.inf for LoadDefaultTemplates • updated 'Terminology' section • updated 'Digital Signing' and 'Buying from Amazon' diagrams • updated the 'Algorithms' section
1.19	4/28/2016	• moved when to disable 'Authenticated Users' from requesting certificates, and that Enterprise PKI will show the sub/policy/issuing CA as broken until that setting is reverted
1.20	4/2/2019	• updated the certificate chaining diagram • updated the hash, symmetric, and asymmetric algorithms
1.21	4/11/2019	• improved comments in CAPolicy.inf files regarding renewal, default templates, AIA extensions, CDP extensions, AlternateSignatureAlgorithm, all thanks to input from Mark B. Cooper of PKISolutions.com
1.22	4/29/2019	• fixed minor text errors that referred the reader to the root CA's CAPolicy.inf file instead of its CertUtil commands file • added the term 'publish' to the glossary • changed the header colors of several sections from grey to yellow so the reader would verify configurations • added information on what the 'Cert Publishers' group is for
1.23	7/19/2019	• added steps for advanced audit policy configuration, and added that information to the CertUtil.exe files • clarified verbiage in the sub/policy/issuing CAPolicy.inf around default template use

		• added 2016, and 2019 to the abstract, and the sub/policy/issuing CAPolicy.inf file in the PathLength section • changed the 'double escaping' steps to include only the CDP directory, and added and explanation of what double escaping is • edited the OID section to read CP (singular) and CPs (plural) instead of 'policies', to better distinguish them from Application Policies • removed the %1_ from the CertUtil.exe files, and added comments where it appears in the screenshots • clarified verbiage in glossary for the terms reissue and renewal
1.24	9/23/2019	• changed the IIS directory and the Sub/Pol/Issuing CA's CAPolicy.inf to indicate Certificate Policy instead of Certification Practice Statement • added a section on SMTP Exit Module
1.25	2/29/2020	• fixed CP and CPS typos and verbiage in PKI Terminology section, and throughout the document

Freeware License and Disclaimer:

(jump to TOC)

About the Author:

(jump to TOC)

Daniel L. Benway

Active Directory, Windows Infrastructure, and Information Security Engineer/SME/Architect

BSc CS, MCSE (2000 & NT4), MCTS (SCCM 2012), CISSP, Security+, Network+, CCNA (2.0), CLP (AD R4)

LinkedIn http://www.LinkedIn.com/in/DanielLBenway

Blog http://www.DanielLBenway.net

twitter @Daniel_L_Benway

Special Thanks:

(jump to TOC)

- Special thanks to Mark B. Cooper (of www.PKISolutions.com) for taking time out of his busy schedule to answer a question I had on the GUI checkbox codes used in Komar's book and in the CertUtil.exe commands of this document, as well as providing improvements to my CAPolicy.inf files.
- Special thanks to Chris Delay (of www.Microsoft.com and http://blogs.technet.com/b/xdot509) for taking time out of his busy schedule to answer a question I had on CRL Overlap periods.
- Special thanks to Brandon Schreiber for pointing out errors, and places for improvement in the document.

Table of Contents:

Warnings:

(jump to TOC)

Be sure to check the revision history of this document to ensure you have the most recent version, and to see what updates, additions, and corrections have been made.

This is an incredibly long document with a few hundred screenshots! I included all of these screenshots so that you could see many of the different areas where PKI is configured, and you could also see the changes as they happened. However, if you just pay attention to the yellow and red highlighted headings from the table of contents you can move through this document pretty quickly.

Grey highlights in the TOC are low priority, usually informational topics
Yellow highlights in the TOC are medium priority, usually special information or things to verify
Red highlights in the TOC are high priority, usually steps to perform

Note also that because the CAPolicy.inf and Certutil.exe files have been updated since initial publication of this document, the values in the screenshots (such as registry settings, publication intervals, etc.) might not always reflect the values from those files.

Other Helpful Info:

(jump to TOC)

servers:

DLBT-ADDS1	Domain Controller 1
DLBT-ADDS2	Domain Controller 2
DLBT-PKI1	Root CA, offline workgroup member
DLBT-PKI2	Sub/Policy/Issuing CA, online Domain member

nomenclature:

RC = right click
RCC = right double click
RD = right drag
LC = left click
LCC = left double click
LD = left drag

PKI Terminology:

(jump to TOC)

- **Asymmetric Key Cryptography** - a.k.a. public-key cryptography - an encryption system which uses two separate keys, one made public and the other kept private, either of which can be used to encrypt data while only the other one can be used to decrypt it. Oftentimes asymmetric key cryptography is used to secretly share a totally different single key (a session key) amongst communication partners who will then use that different single key to encrypt all further communication using symmetric key cryptography. Asymmetric key cryptography is slower than symmetric key cryptography.
- **AIA** - Authority Information Access - a URL (local file path, remote file share, LDAP, or HTTP) which specifies where a specific CA's certificate is available for use in certificate chaining.
    - The AIA extension on a CA specifies the AIA information that will be put into the certificates that said CA issues. Said AIA information points to where said CA's certificate is published.
    - The AIA information within a certificate points to where the signer of said certificate has its CA certificate published.
- **Auto-Enrollment** - the mechanism by which a subject automatically requests and is issued certificates from a CA.
- **CDP** - CRL Distribution Point - a URL (local file path, remote file share, LDAP, or HTTP) which specifies where a certificate's CRL is available.
    - The CDP extension on a CA specifies the CDP information that will be put into the certificates that said CA issues. Said CDP information points to where said CA will publish CRLs for the certificates it issues.
    - The CDP information within a certificate points to where the signer of said certificate will publish that certificate's CRL.
- **CA** - Certification Authority - a trusted computer and/or organization that issues certificates to subjects.
- **Certificate** - a file that is signed by a CA, and contains descriptive and identifying information about a person or computer (the subject), and contains that person's or computer's public key.
- **Certificate Chaining** - using AIA, CDPs, and CRLs to verify each certificate between a given certificate and its root to ensure each certificate in the chain to the root is current and true. Only the root CA (the trust anchor) is trusted whereas every intermediate CA and certificate is chained to verify veracity. A certificate contains the CDP URLs and AIA URLs which point to that certificate's CRL (which is published by the certificate's signing CA) and that certificate's issuing CA's certificate respectively.
- **CP** - Certificate Policy - see RFC 3647 - a higher-level document describing what levels of assurance the certificates from a PKI adhere to. A Certificate Policy is represented in a certificate by a unique number called an "Object Identifier" (OID), which is specified in the CAPolicy.inf file on the policy CA which governed the certificate's issuance (which in a 2-tier PKI are the subordinate/policy/issuing CAs). Refer to the sub/policy/issuing CA's CAPolicy.inf file in this document for an example.
- **CPS** - Certification Practice Statement - see RFC 3647 - a lower-level document describing how the CAs of a PKI are managed.
- **CRL** - Certificate Revocation List - a file, managed by a particular CA, which contains the revocation status of all certificates issued by that particular CA (so CRLs are per CA, not per certificate).
- **Cross-signing / cross certification** - a certificate can only be signed by exactly one CA. In a 2-tier PKI, cross signing is where a sub/policy/issuing CA holds multiple CA certificates for itself (all with the same public key) each signed by a different root CA. This way there are multiple certification paths between an end certificate and a trusted root. This accomplishes two things: it expands the PKI to include multiple trust anchors (from, say, different organizations), and it also provides root redundancy in case a root is compromised.
- **CSR** - Certificate Signing Request - a request from a subject to a CA for a certificate. A CSR contains the subject's descriptive and identifying information, and also contains the subject's public key. See 'Enrollment'.

- **Digest** - see 'Hash Function'.
- **Digital Signing** - the following steps explain digital signing by example:
    - A subject hashes data (or a file) to create a digest.
    - The subject encrypts the digest using the subject's own private key (the private key encrypted digest is the signature).
    - The subject includes the signature with the data and sends it all to the recipient.
    - The recipient of the data and signature decrypts the signature using the subject's public key.
    - The recipient hashes the received data.
    - The recipient compares the digest it generated against the digest the subject provided.
    - If the two digests match, the recipient knows that the data came from the subject, and its contents have not been altered.

  (Note that some people sloppily refer to just the asymmetric encryption of the digest as 'signing' and thus refer to asymmetric encryption algorithms as 'signing algorithms'.)
- **DRA - Data Recovery Agent** - an account that can decrypt EFS or BitLocker encrypted data
- **Enrollment** - the process by which a subject generates its own public/private key pair, then sends a CSR to a CA which then creates, signs, and issues to the subject a certificate which contains the subject's descriptive and identifying information, and also the subject's public key.
- **Enterprise CA** - a CA that is a domain member of a Microsoft Active Directory
- **Fingerprint** - the digest of a public key
- **Hash Function** - a one-way mathematical function that processes information of arbitrary length to produce a different, fixed-length result (called a digest) that is almost always unique to the original input information.
- **Install** - to take a certificate for which you or your machine is not the subject and save it into your local certificate store for fast access in the future.
- **Issue:**
    - With reference to a certificate, issuing is when a CA signs a CSR from a subject and gives a certificate to the requesting subject. See 'Enrollment'.
    - With reference to a template, issue means to enable the template for usage on a CA.
        - from my test lab it looks like templates are issued from a particular CA, and the issuance only affects that particular CA (i.e. a template issued on an enterprise sub CA doesn't show up as issued on the enterprise root CA)
- **Issuing CA** - although every CA issues certificates, an 'issuing CA' is generally considered to be one that issues certificates to the end entities (like users, workstations, web servers, etc.).
- **KRA - Key Recovery Agent** - an account that can recover private keys for certificates issued by a CA
- **OID** - Object Identifier - a hierarchical, numerical designator that is used to specifically name an item (such as a policy in your PKI, or an attribute in your Active Directory).
- **Overlap** - the amount of time a base or delta CRL can be used after it has expired.
- **Policy CA -** a policy CA contains legal documents and statements about the PKI, and it contains configuration settings that control the PKI (by controlling itself and its subordinate CAs, if any). In a single-tier PKI, the root CA is the policy CA, but in a multi-tier PKI, the policy CA(s) is(are) immediately underneath the root CA.
- **Public Key Cryptography** - a.k.a. Asymmetric Key Cryptography
- **Rainbow Table** - tables of common data and their corresponding digests, used to ascertain original data given its digest
- **Reissue** - the process by which a subject enrolls for a new certificate to replace a revoked one, with a new private/public key pair. This term is sometimes confused with 'renewal'.

- **Renewal** - the process by which a subject enrolls for a new certificate to replace an expiring one, oftentimes with the same private/public key pair. This term is sometimes confused with 'reissue'.
- **Revoke** - to make a certificate invalid by rescinding its authority (by publishing its deprecated status in a Certificate Revocation List, or by using Online Certificate Status Protocol (OCSP).
- **Root CA -** a root CA is the trust anchor of a PKI, its certificate is self-signed, and the CA is considered a trusted root certification authority by the entities that use the PKI.
- **Sign** - the act of adding a digital signature to a file. See 'Digital Signing'.
- **Stand-alone CA** - a CA that is a workgroup member, not a domain member of a Microsoft Active Directory domain
- **Subject** - a person or computer to which a certificate is associated, whose identity the certificate proves, and to which the certificate's public key belongs (which corresponds to the private key that the subject holds confidential).
- **Subordinate CA** - a subordinate CA is one which has a parent (a CA immediately above it) in the PKI hierarchy which has signed the subordinate CA's CA certificate.
- **Symmetric Key Cryptography** - a.k.a. secret-key encryption - an encryption system which uses a single key, which is kept private amongst communication partners, to both encrypt and decrypt data. Symmetric key cryptography is faster than asymmetric key cryptography.
- **Template** - different certificates are based on different templates, just like different databases are based on different schemas. Only Enterprise CAs use templates, stand-alone CAs configure the certificates they issue by using the data in their own registries and the data contained in the associated CSR.
- **Thumbprint** - see 'fingerprint'
- **Trust** - a root CA is trusted, and its CA certificate is thus in your local trusted store. Everything below it is AIA chained to establish veracity.

https://technet.microsoft.com/en-us/library/cc753754.aspx

- **Certification authorities (CAs)**. A CA accepts a certificate request, verifies the requester's information according to the policy of the CA, and then uses its private key to sign the certificate. The CA then issues the certificate to the subject of the certificate for use as a security credential within a PKI. A CA is also responsible for revoking certificates and publishing a certificate revocation list (CRL).

- **CA certificates**. A CA certificate is a certificate issued by a CA to itself or to a second CA for the purpose of creating a defined relationship between the two CAs. A certificate that is issued by a CA to itself is referred to as a trusted root certificate. CA certificates are critical to defining the certificate path and usage restrictions for all end-entity certificates issued for use in the PKI.

- **Authority information access locations**. Authority information access locations are URLs that are added to a certificate in its authority information access extension. These URLs can be used by an application or service to retrieve the issuing CA certificate. These CA certificates are then used to validate the certificate signature and to build a path to a trusted certificate.

- **CRLs**. CRLs are complete, digitally signed lists of unexpired certificates that have been revoked. This CRL is retrieved by clients who can then cache the CRL (based on the configured lifetime of the CRL) and use it to verify certificates presented for use.

- **CRL distribution points**. CRL distribution points are locations, typically URLs, that are added to a certificate in its CRL distribution point extension. CRL distribution points can be used by an application or service to retrieve a CRL. CRL distribution points are contacted when an application or service must determine whether a certificate has been revoked before its validity period has expired.

https://technet.microsoft.com/en-us/library/cc753754.aspx

- **Certification authorities (CAs)**. A CA accepts a certificate request, verifies the requester's information according to the policy of the CA, and then uses its private key to sign the certificate. The CA then issues the certificate to the subject of the certificate for use as a security credential within a PKI. A CA is also responsible for revoking certificates and publishing a certificate revocation list (CRL).

- **CA certificates**. A CA certificate is a certificate issued by a CA to itself or to a second CA for the purpose of creating a defined relationship between the two CAs. A certificate that is issued by a CA to itself is referred to as a trusted root certificate. CA certificates are critical to defining the certificate path and usage restrictions for all end-entity certificates issued for use in the PKI.

- **Authority information access locations**. Authority information access locations are URLs that are added to a certificate in its authority information access extension. These URLs can be used by an application or service to retrieve the issuing CA certificate. These CA certificates are then used to validate the certificate signature and to build a path to a trusted certificate.

- **CRLs**. CRLs are complete, digitally signed lists of unexpired certificates that have been revoked. This CRL is retrieved by clients who can then cache the CRL (based on the configured lifetime of the CRL) and use it to verify certificates presented for use.

- **CRL distribution points**. CRL distribution points are locations, typically URLs, that are added to a certificate in its CRL distribution point extension. CRL distribution points can be used by an application or service to retrieve a CRL. CRL distribution points are contacted when an application or service must determine whether a certificate has been revoked before its validity period has expired.

Buying from Amazon

1. Amazon needs a certificate to prove to the world that it is who it claims to be, and to encrypt its communication with its customers (these are the two critical purposes of a certificate). First, Amazon generates a private/ public key pair (this is asymmetric key cryptography).

2. Amazon sends its public key to VeriSign (in a certificate signing request).

AmazonPub
AmazonPvt

3. After performing appropriate investigations and verifications of Amazon (and charging a veritable boatload of money), VeriSign creates and digitally signs a certificate containing Amazon's public key, and sends this certificate to Amazon. This certificate proves to the world that VeriSign vouches for Amazon. Amazon will use this certificate for months or years.

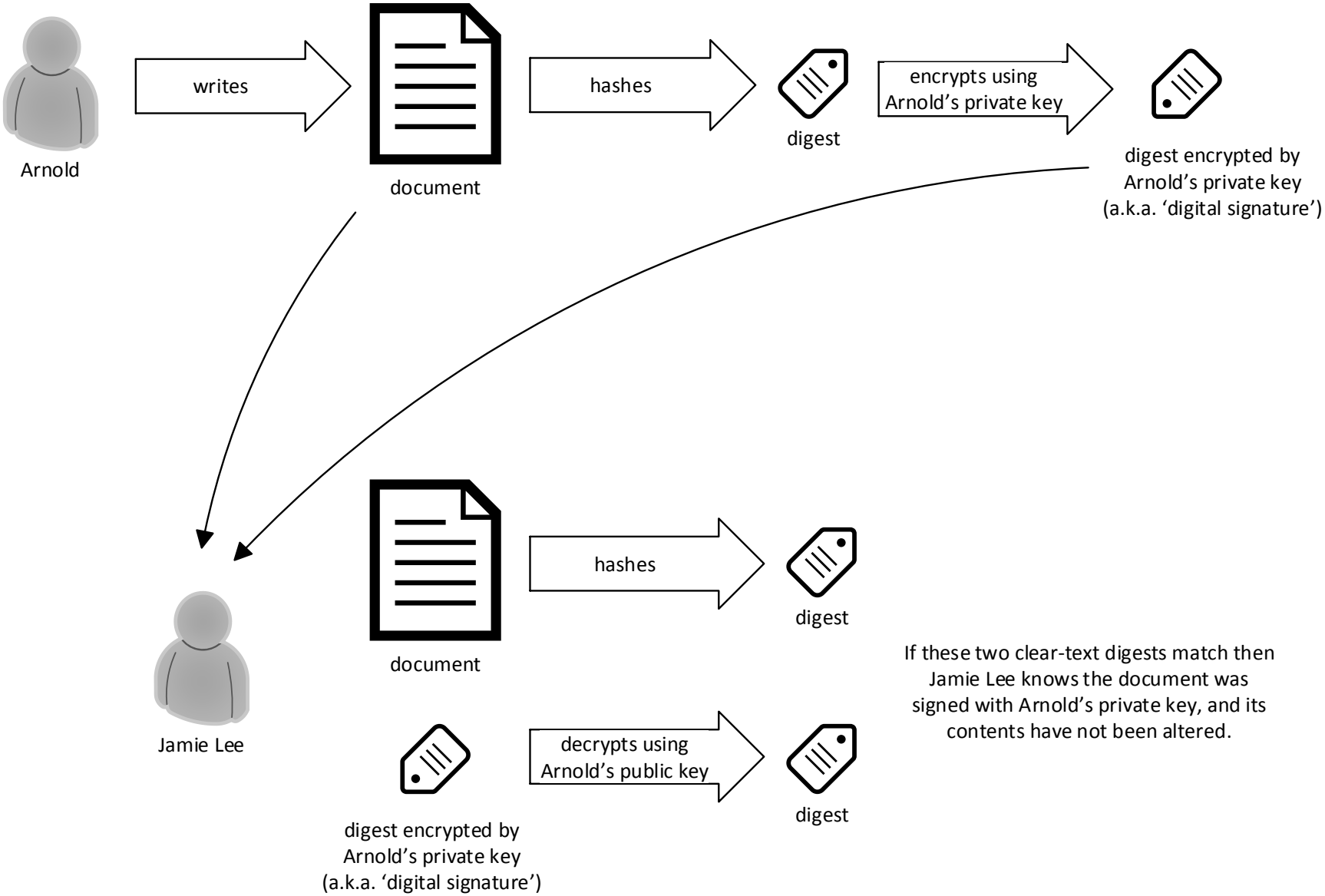
4. A customer wants to buy a book from Amazon. The customer's browser downloads Amazon's certificate (from Amazon) which contains Amazon's public key. (The customer can verify the certificate is both unaltered and also signed by VeriSign by using VeriSign's public key to decrypt VeriSign's digital signature on said certificate.)

5. The customer's browser generates a short-term, per-session, symmetric key, encrypts it with Amazon's public key, and sends it to Amazon.

Customer

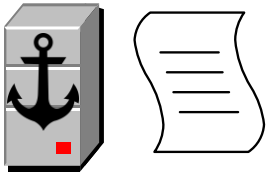
6. Amazon receives the symmetric key (encrypted with Amazon's public key) from the customer's browser, decrypts it using Amazon's private key, then uses that symmetric key to encrypt all further communication between Amazon and the customer (this is symmetric key cryptography). Amazon and the customer will use this symmetric key for the duration of their shared browser session.

Digital Signing



Certificate Chaining in a 2-Tier PKI

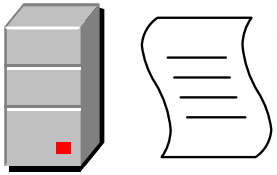
<u>root CA</u>
-contains this CA's private key
-CDP extensions point to where this CA will publish its CRL for all of the certificates it issues (except its own, self-signed certificate), the location is written into said certificates
-AIA extensions point to where this CA's certificate is published, the location is written into the certificates this CA issues



<u>root CA's CA certificate</u>
-signed by root CA (i.e. self-signed)
-contains root CA's public key (key length set in ADCS wizard)
-validity period set in ADCS wizard
-renewal parameters set in CAPolicy.inf
-CDP information
. contains no CDP information
. configured from root CA's CAPolicy.inf
. there's no higher CA that would publish a CRL which would control this certificate
. root CA's certificate is normally not revocation checked
-AIA information
. contains no AIA information
. configured from root CA's CAPolicy.inf
. there's no higher CA whose certificate and signature would be checked

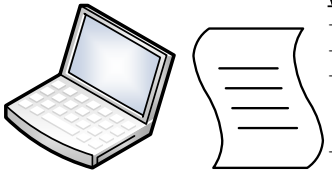
---

<u>sub/policy/issuing CA</u>
-contains this CA's private key
-CDP extensions point to where this CA will publish its CRL for all of the certificates it issues, the location is written into said certificates
-AIA extensions point to where this CA's certificate is published, the location is written into the certificates this CA issues



<u>sub/policy/issuing CA's CA certificate</u>
-signed by root CA
-contains sub/policy/issuing CA's public key (key length set in ADCS wizard)
-validity period set in ADCS wizard
-renewal parameters set in CAPolicy.inf
-CDP information
. configured from root CA's extensions
. points to where the root CA publishes its CRL
-AIA information
. configured from root CA's extensions
. points to where root CA's certificate is published

<u>workstation</u>
-contains this workstation's private key
-no CDP extensions
-no AIA extensions



<u>workstation's certificate</u>
-signed by sub/policy/issuing CA
-contains workstation's public key
-CDP information
. configured from sub/policy/issuing CA's extensions
. points to where the sub/policy/issuing CA publishes its CRL
-AIA information
. configured from sub/policy/issuing CA's extensions
. points to where sub/policy/issuing CA's certificate is published

PKI Algorithms:

(jump to TOC)

Note: This is not a complete list.

hash algorithms:

- Tiger
- MD 2, 4, 5
- SHA 0, 1, 2 (and 256), 3
- HAVAL 3, 4
- HMAC
- Whirlpool

symmetric (1 key) encryption algorithms:

- DES, 2DES, 3DES, DESX
- RC 2, 4, 5, 6
- Blowfish, TwoFish, Skipjack
- Serpent
- CAST
- Rijndael (currently the algorithm specified as AES)
- MARS
- SAFER
- IDEA

asymmetric (2 different keys) encryption algorithms (sometimes sloppily called 'signing algorithms', sloppy because signing uses a hash followed by an asymmetric encryption algorithm, not just an asymmetric encryption algorithm)**:**

- LUC
- XTR
- El Gamal
- Diffe-Hellman
- RSA
- ECC (elliptical curve)
- Knapsack
- MQV

signature formats/standards (specify the acceptable parameters and combinations of hash and encryption algorithms used in digital signatures)**:**

- PKCS #1 (Public Key Cryptography Standard #1) - v 2.1 and later are not compatible with XP and 2003

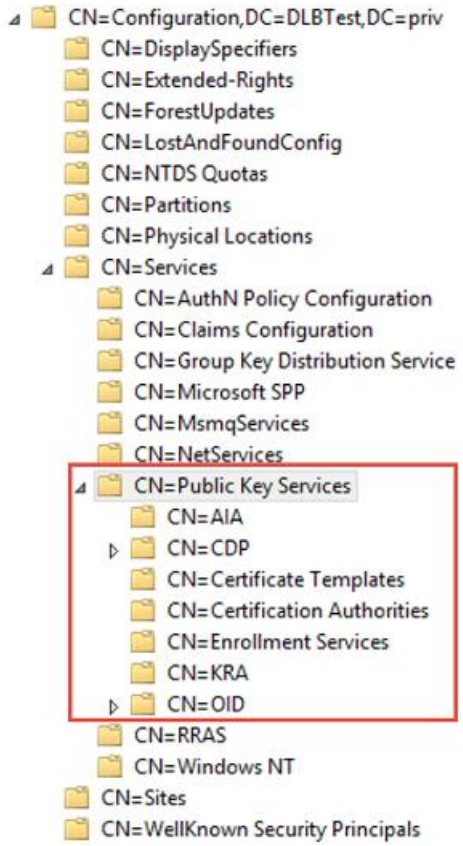
certificate formats/standards:

- X.509 v1, v2, v3, v4

ADSIEdit and PKI:

(jump to TOC)

This is where AD stores PKI information:



Komar p.171

- **AIA** - all CA certificates in the PKI (roots and subs)
- **CDP** - the CDPs in the PKI
- **Certificate Templates** - certificate templates that have been issued into AD
- **Certification Authorities** - root CAs only
- **Enrollment Services** - enterprise CA certificates
- **KRA** - Key Recovery Agent certificates
- **OID** - object identifier definitions for PKI objects (like policies and templates)
- **NTAuthCertificates** - all CAs that can issue certificates for smart cards and RADIUS

CDP Setup:

(jump to TOC)

This heading is just a TOC placeholder.

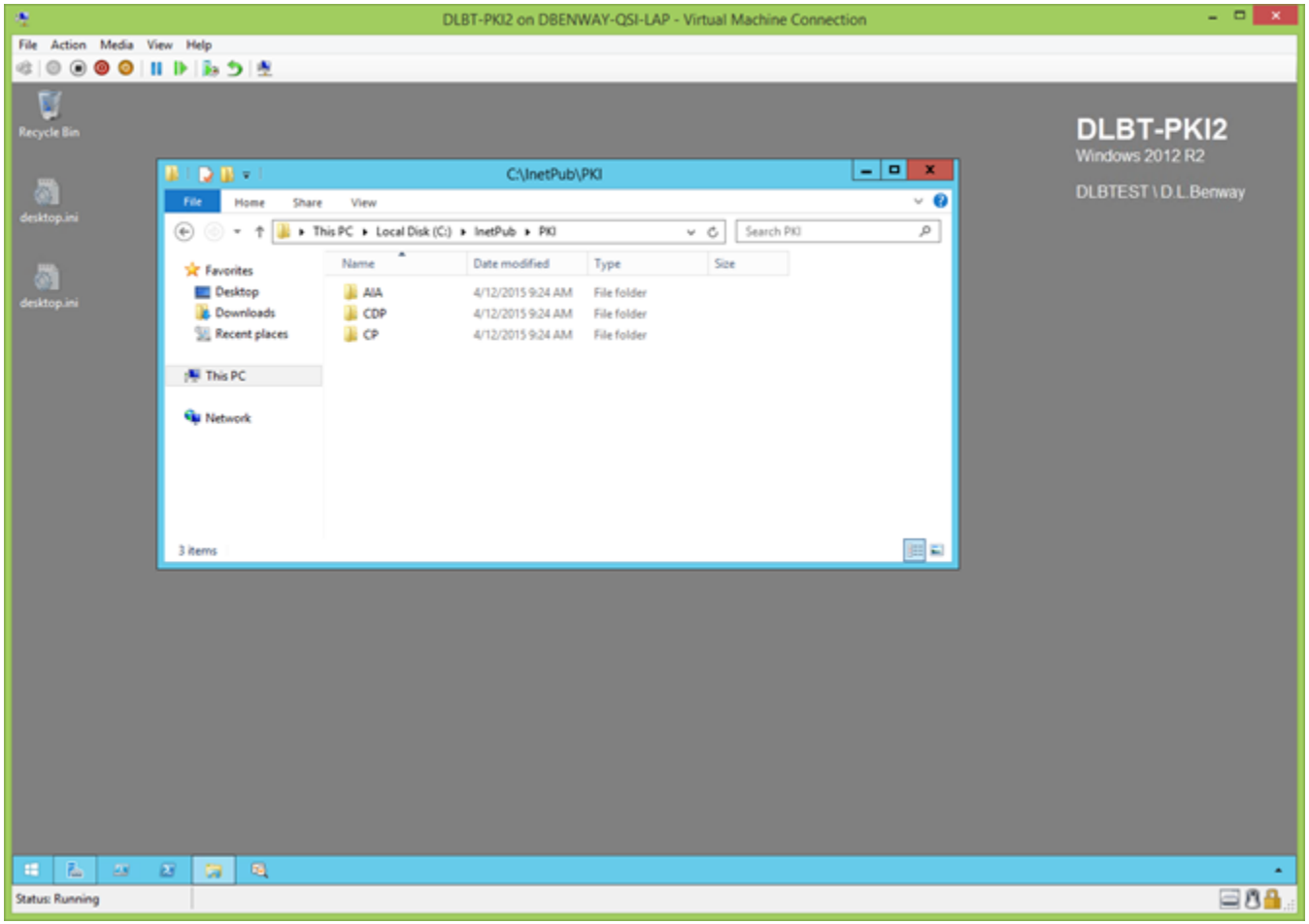
IIS Setup on the CDP:

(jump to TOC)

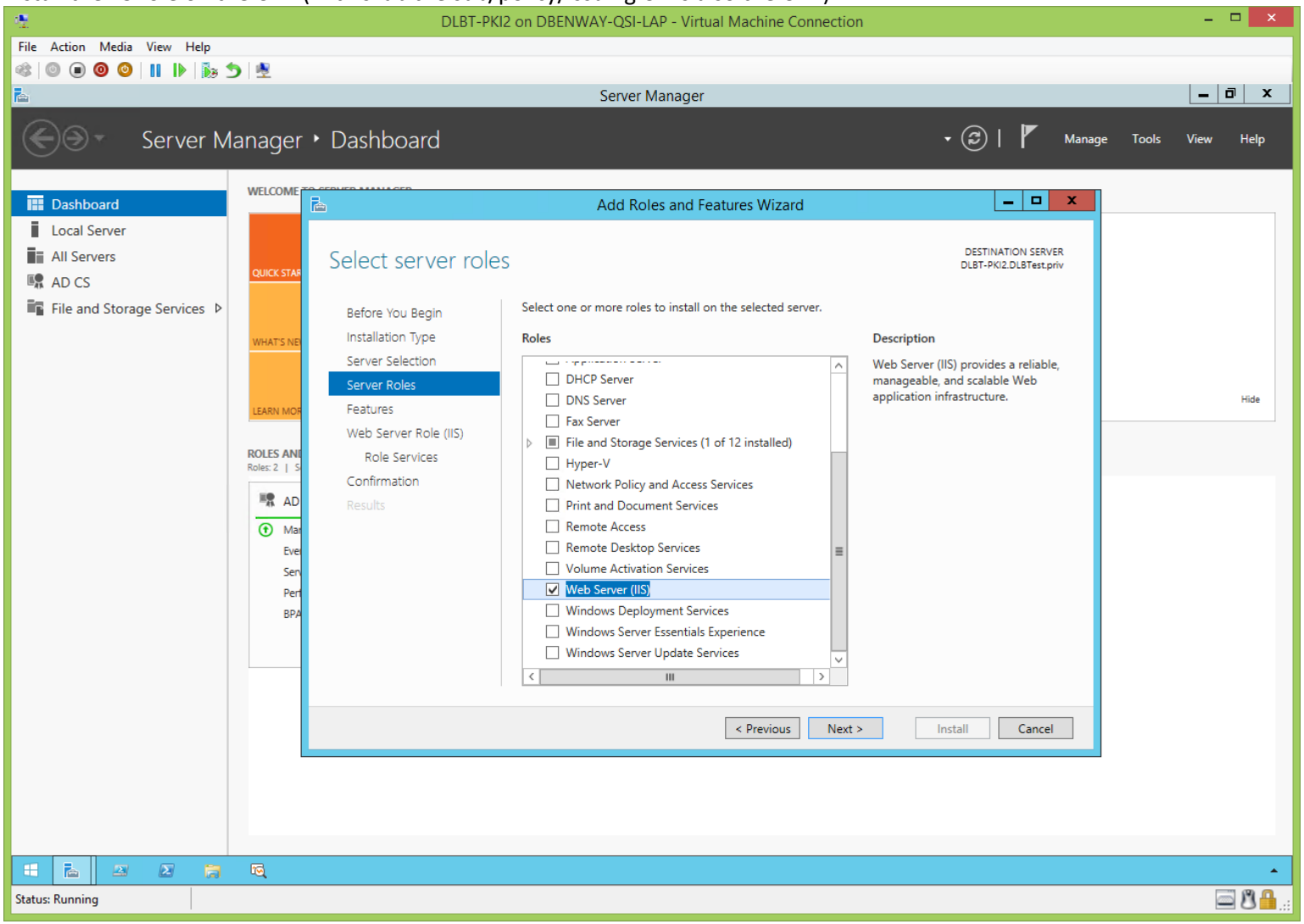
In this lab, the CDP will be put on the sub/policy/issuing CA. On the CDP, setup the directories for AIA, CDP, and CPS in IIS (these are on C: because this is a simple lab environment):

```
mkDir C:\InetPub
mkDir C:\InetPub\PKI
mkDir C:\InetPub\PKI\AIA
mkDir C:\InetPub\PKI\CDP
mkDir C:\InetPub\PKI\CP
```

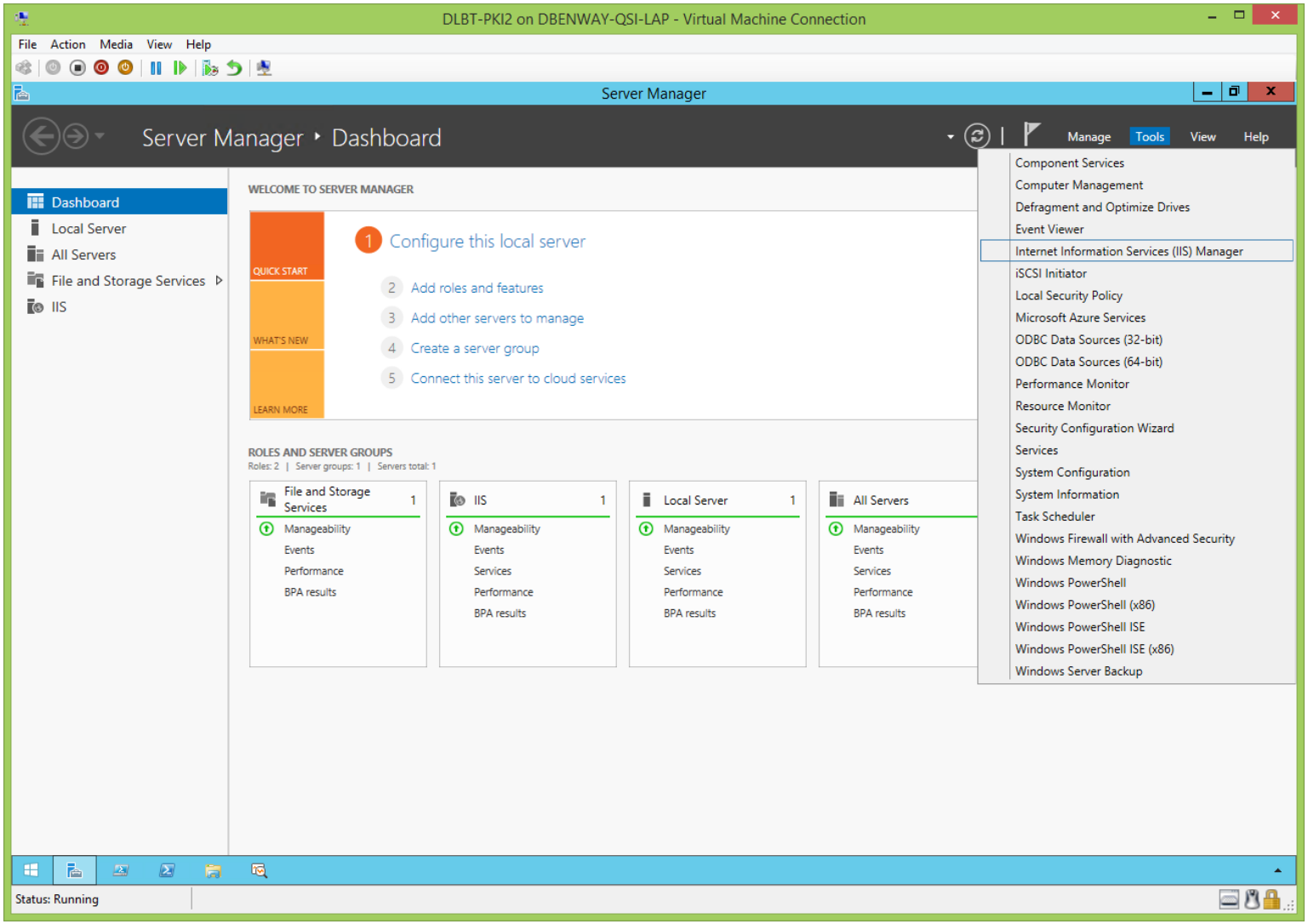
Normally it's poor practice to put a CDP on a CA because it exposes the CA on http. In our case it's OK because this is a small, internal PKI, and because our CNAME will allow us to easily move the CDP to wherever we want if the need arises in the future.



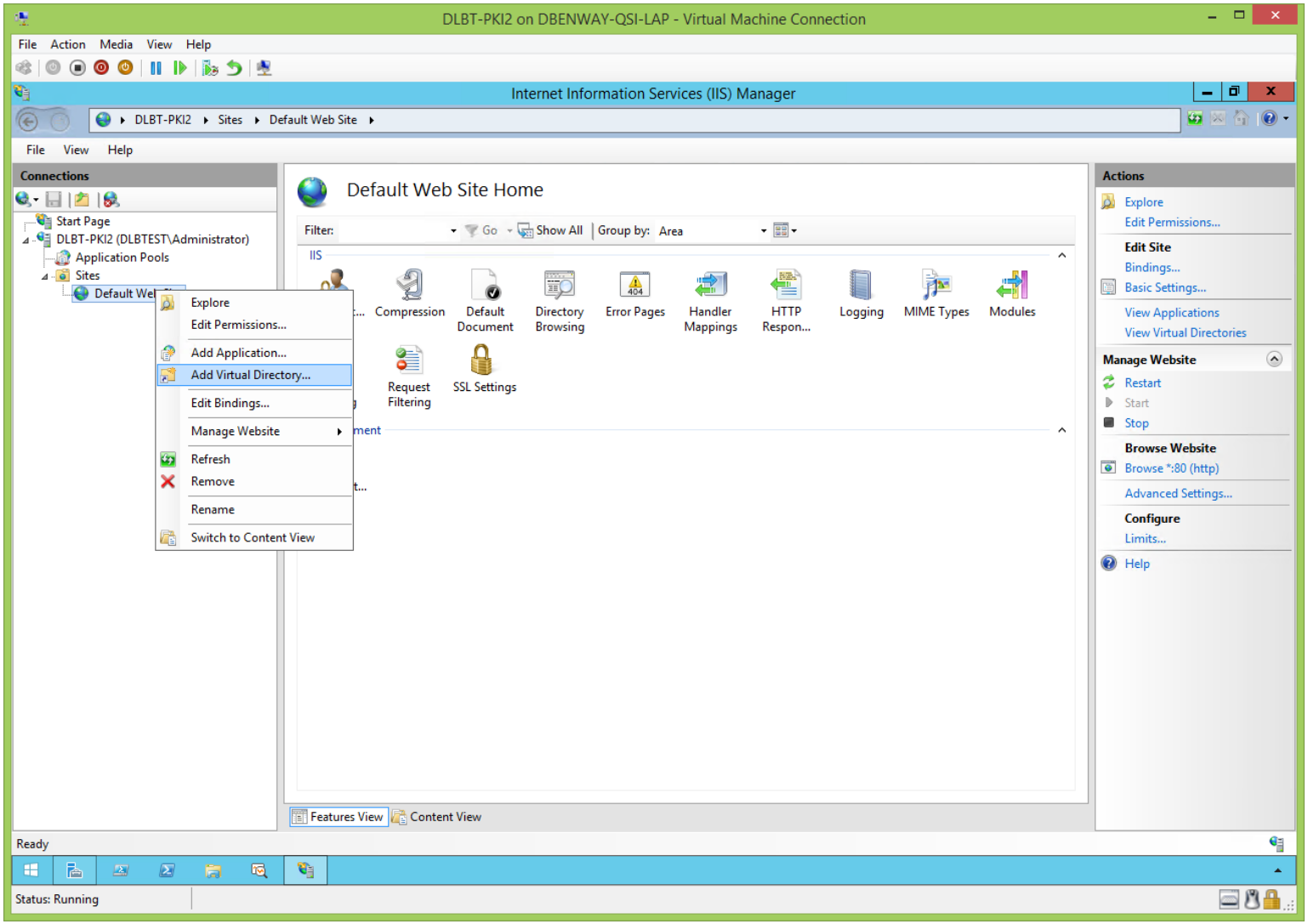
Install the IIS role on the CDP (in this lab the sub/policy/issuing CA is also the CDP):



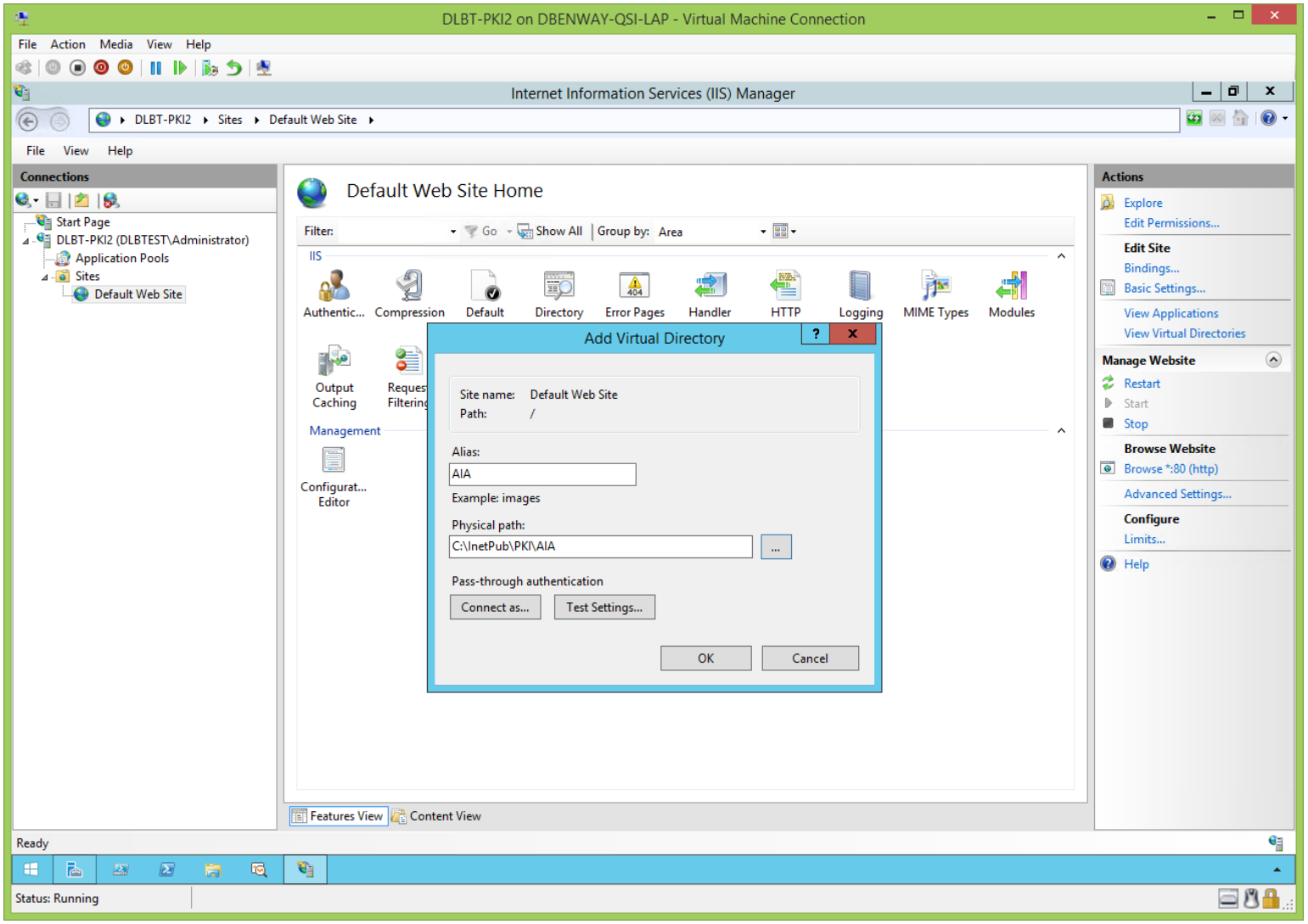
Open IIS Manager:



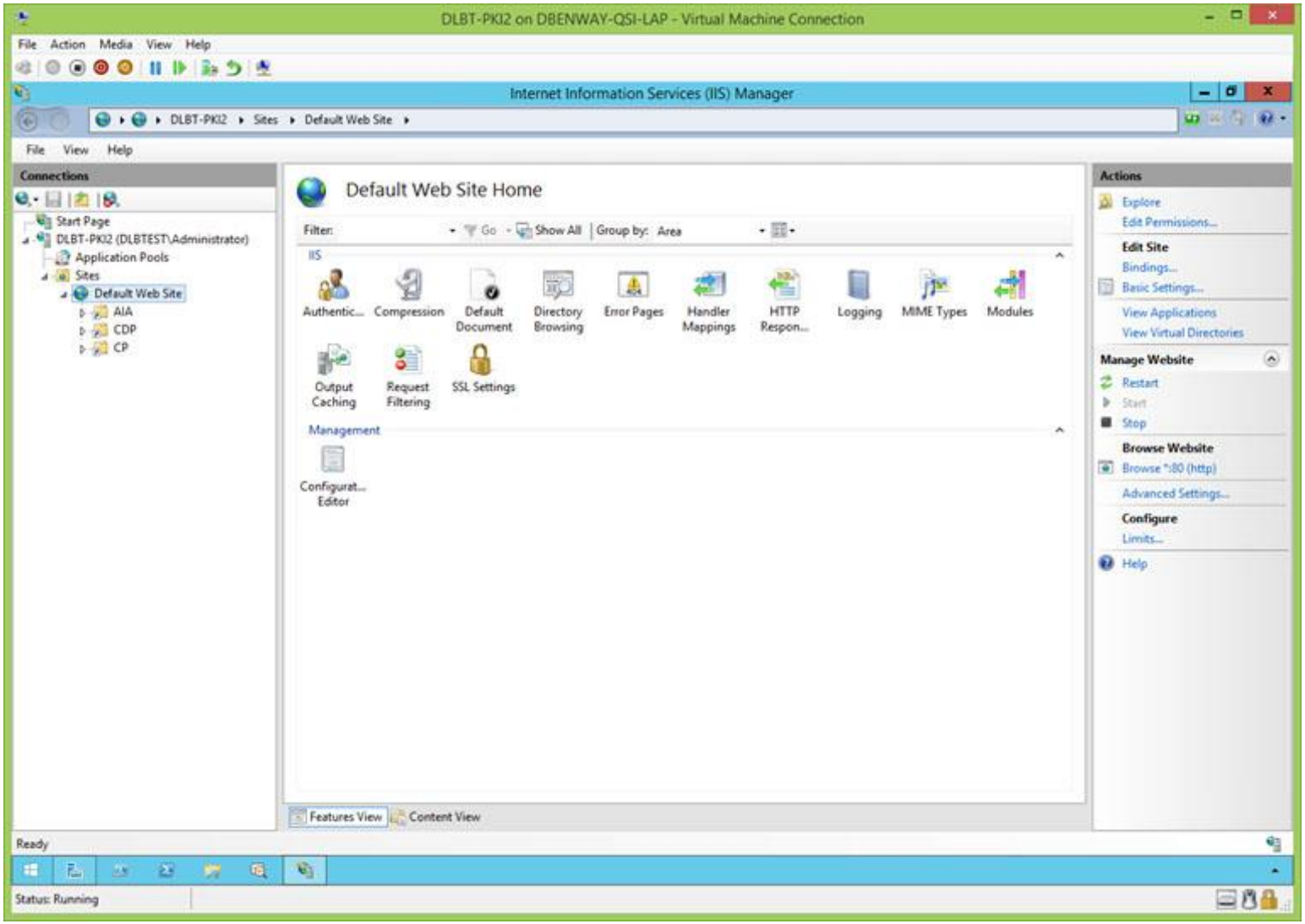
Create a virtual directory named ‘AIA’ with a physical path of ‘C:\InetPub\PKI\AIA’:



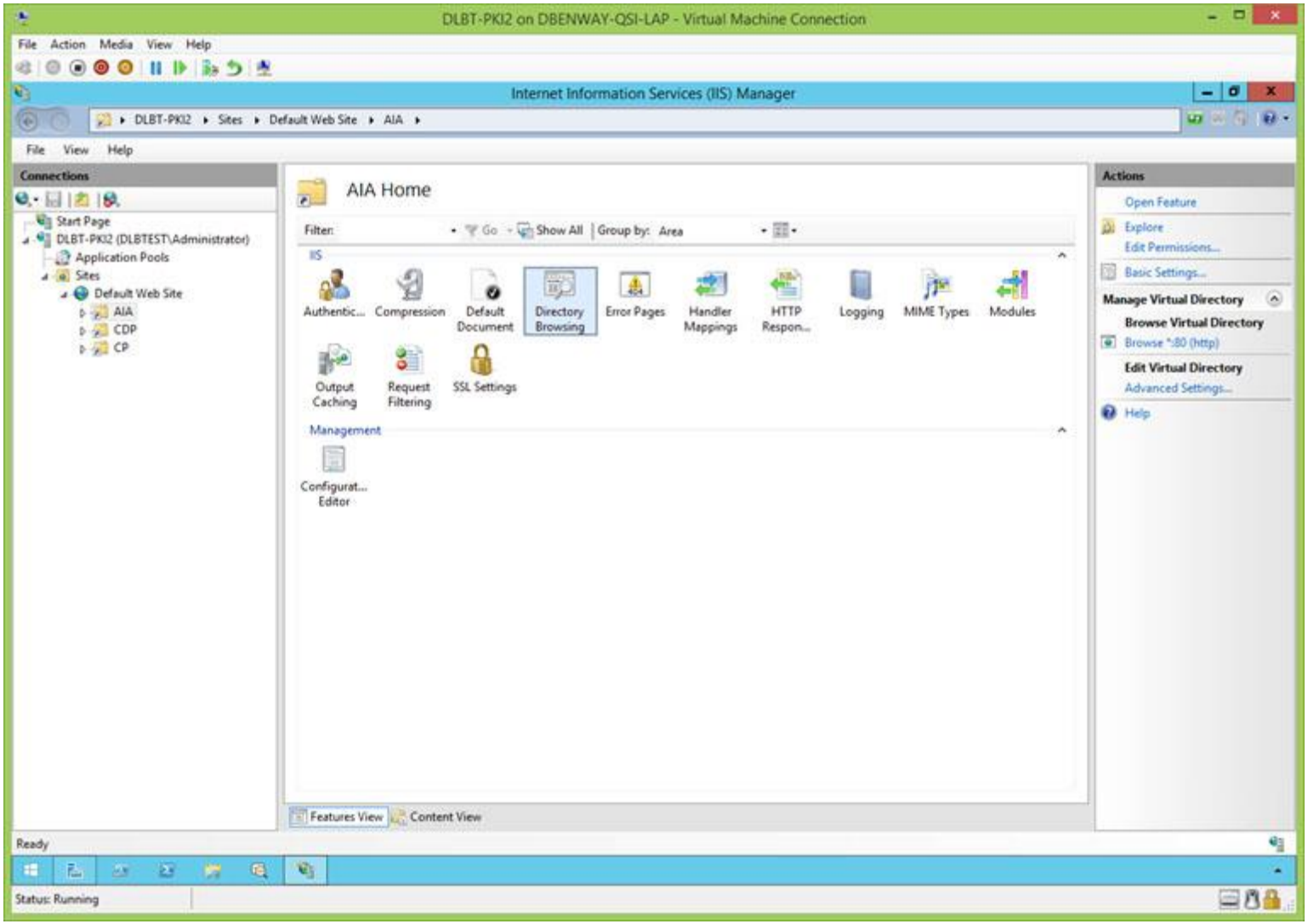
Create a virtual directory, cont'd:



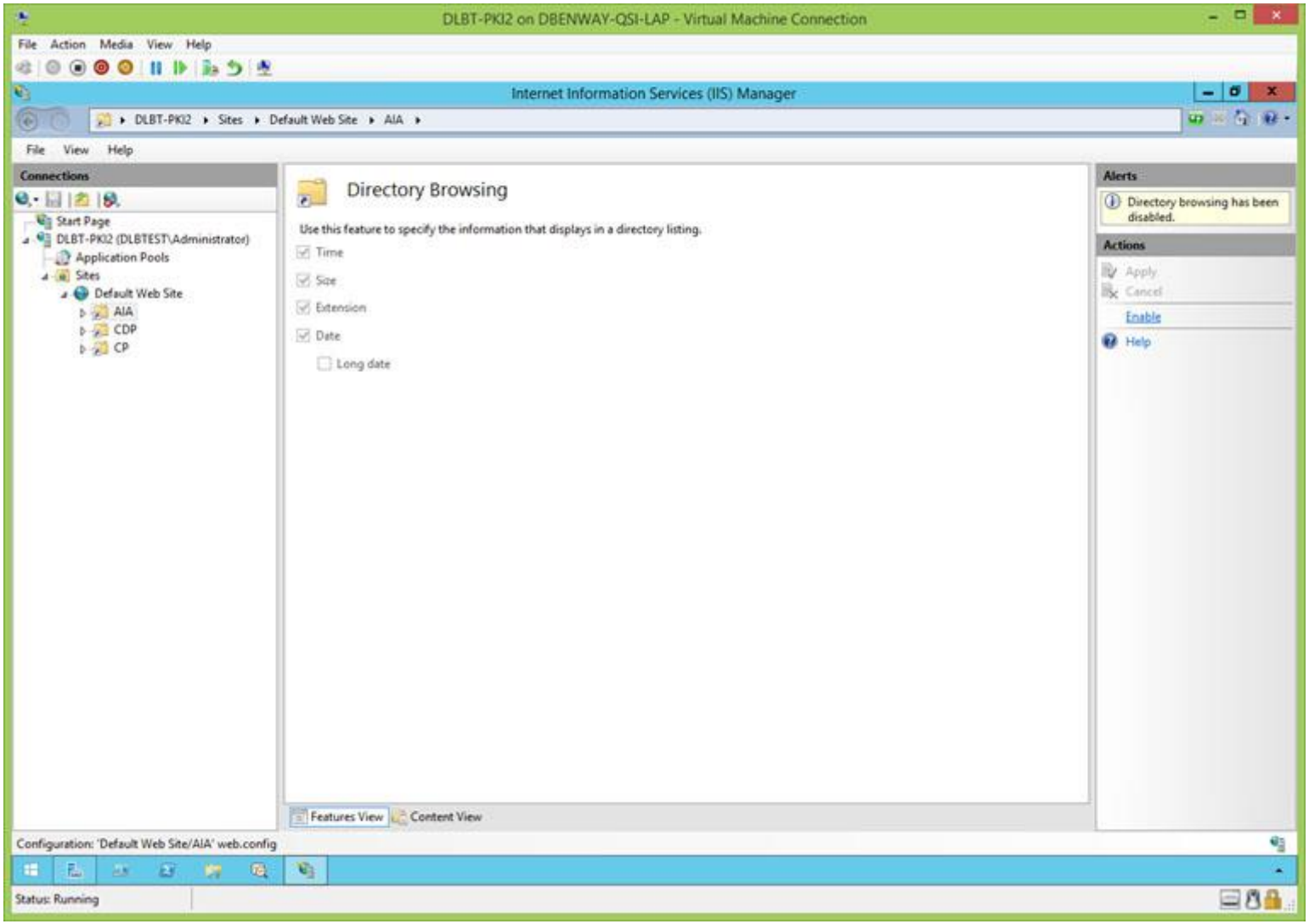
Create virtual directories for CDP, and CP as well (pointing to their respective folders in C:\InetPub\PKI):



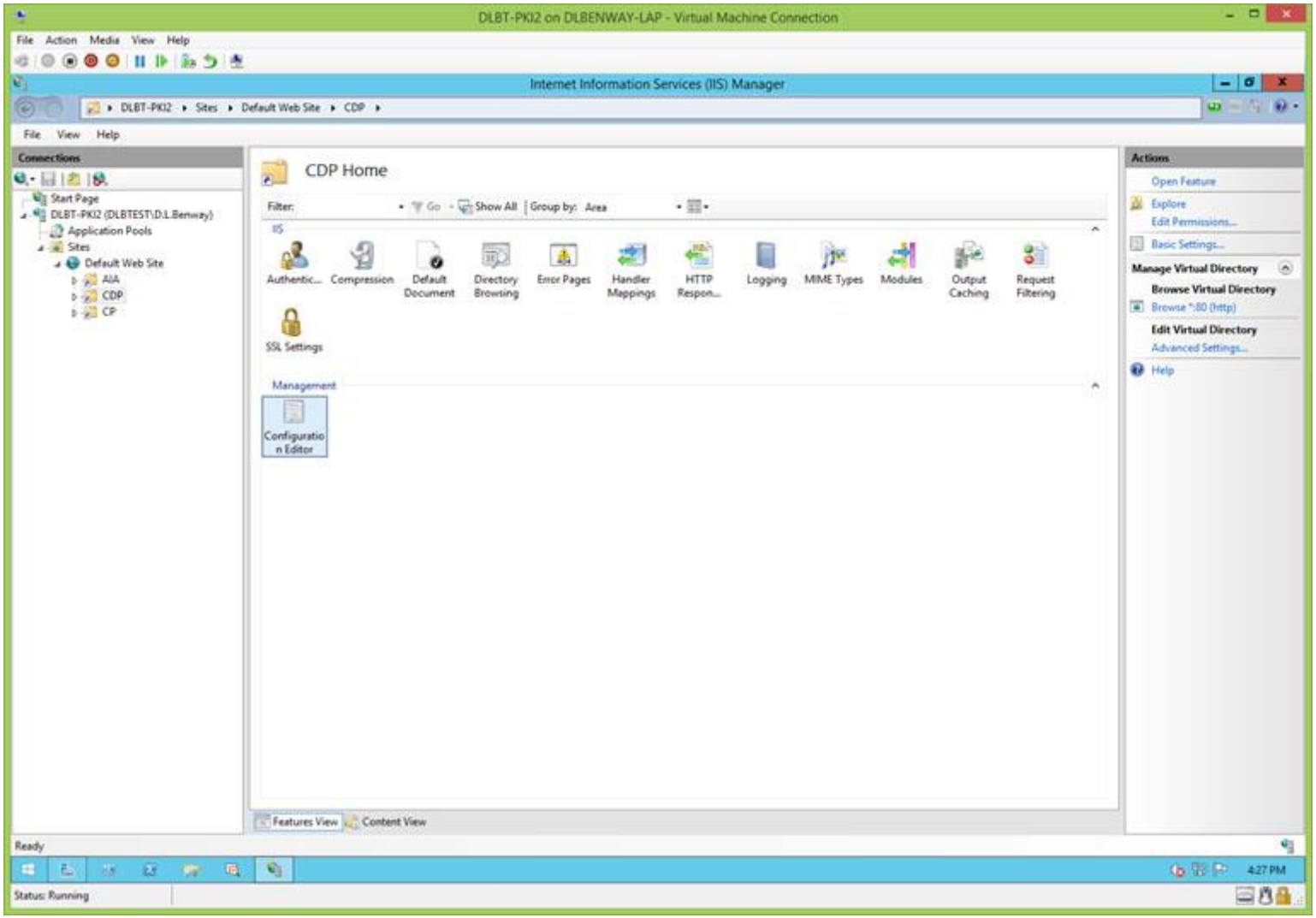
For each of the three virtual directories, go to ‘Directory Browsing’:



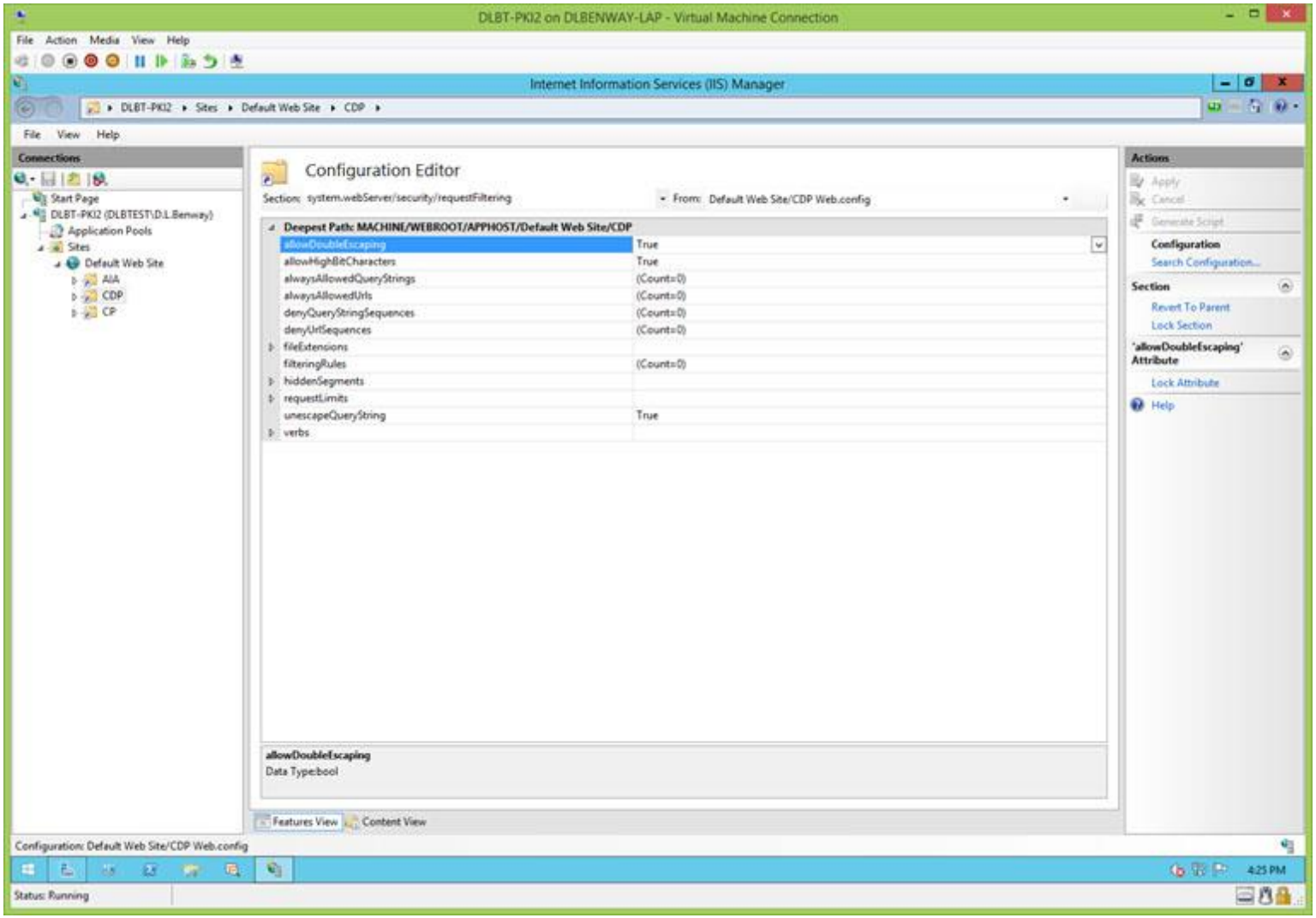
LC ‘enable’ on the right to enable directory browsing:



For the CDP virtual directory go into ‘Configuration Editor’:



Go into section ‘system.webServer/security/requestFiltering’ and change ‘allowDoubleEscaping’ to ‘True’, then LC ‘Apply’ on the right:

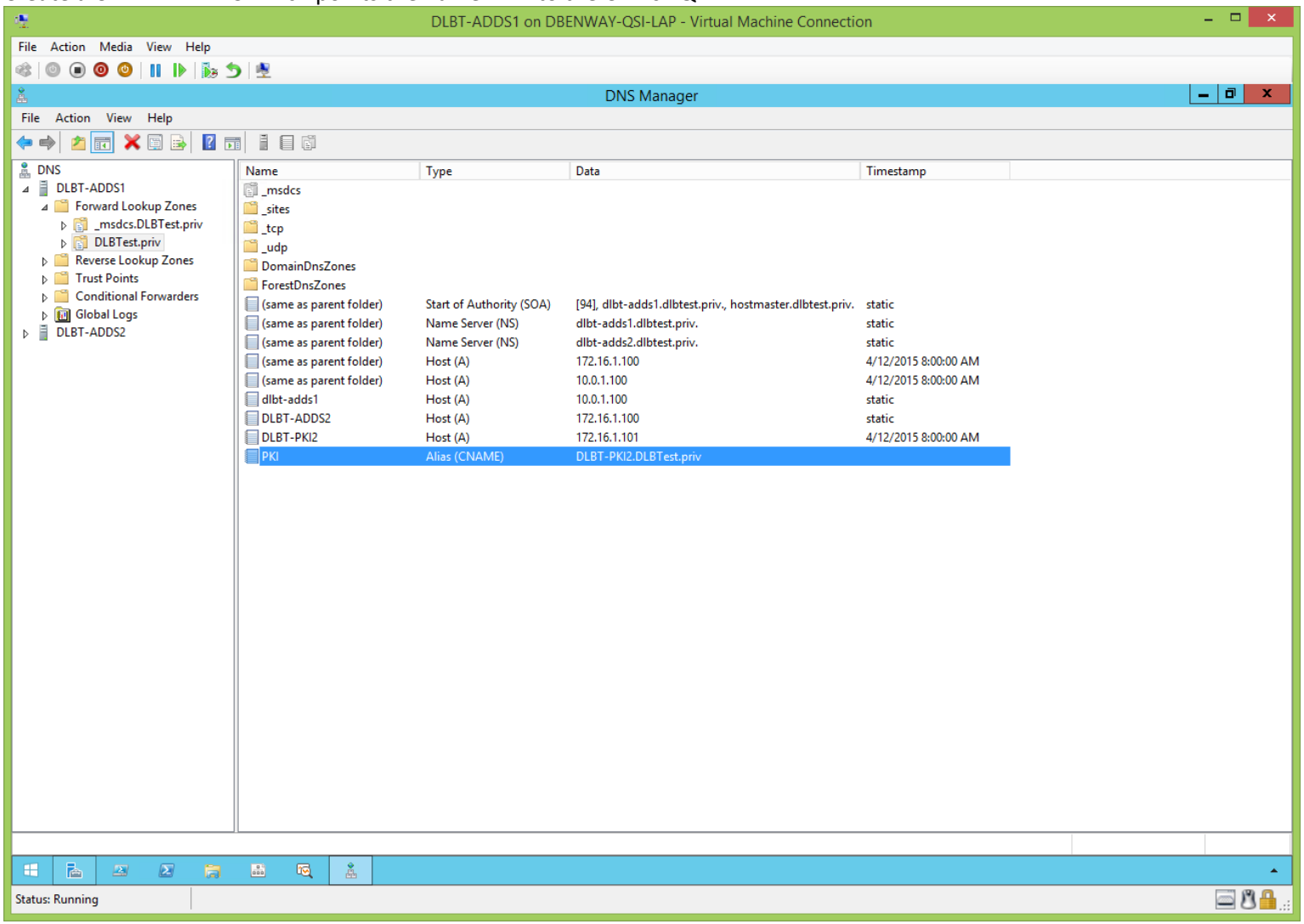


‘Double Escaping’ allows the IIS server to properly offer files whose names contain the plus sign, ‘+’, which delta CRLs do.

DNS Records:

(jump to TOC)

Create a CNAME in DNS which points the name 'PKI' to the CDP's FQDN:

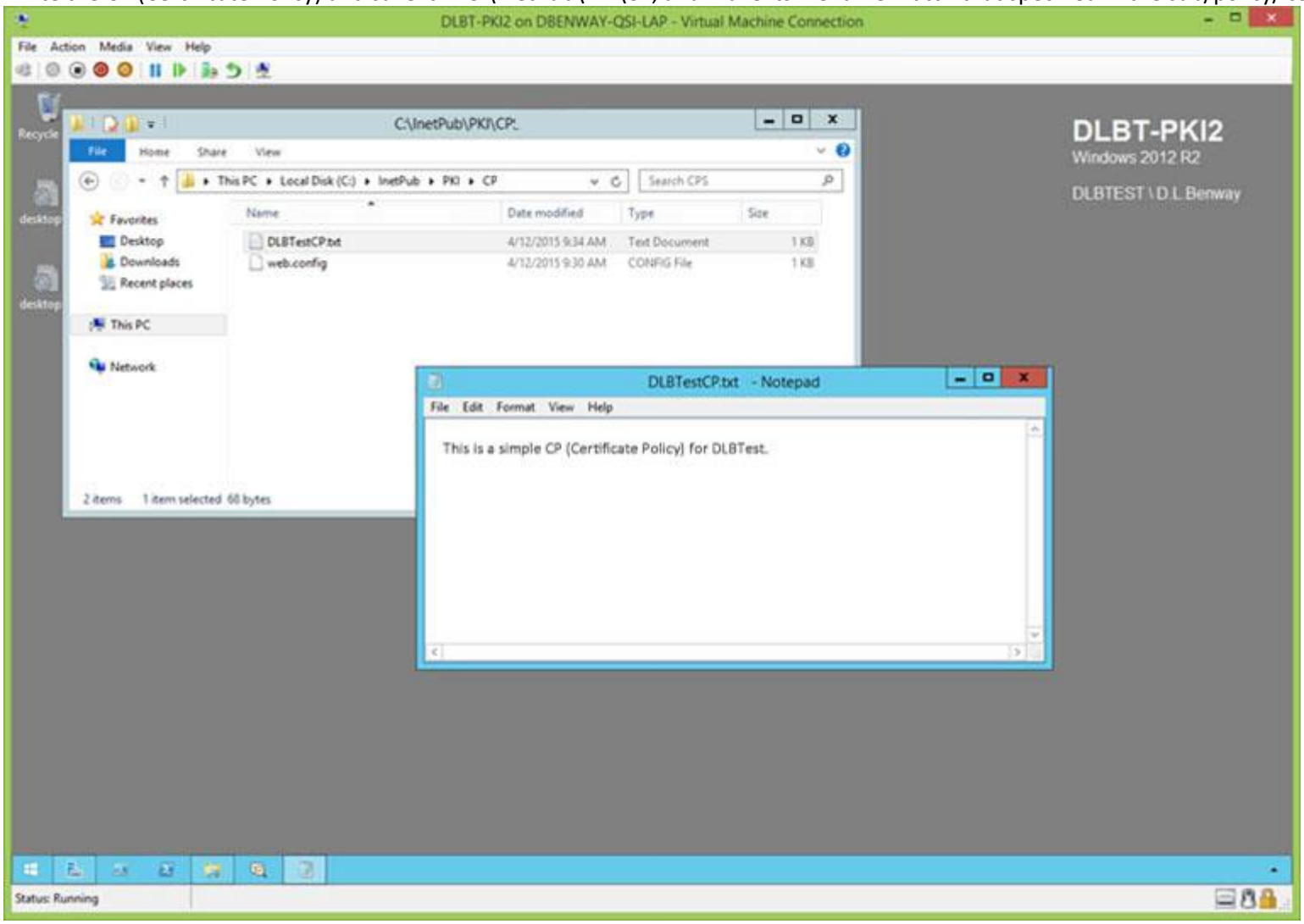


Note: the name 'PKI' was chosen to match that specified in the sub/policy/issuing CA's CAPolicy.inf, and the CertUtil.exe commands run on the root CA and on the sub/policy/issuing CA.

Write and Publish the CP:

(jump to TOC)

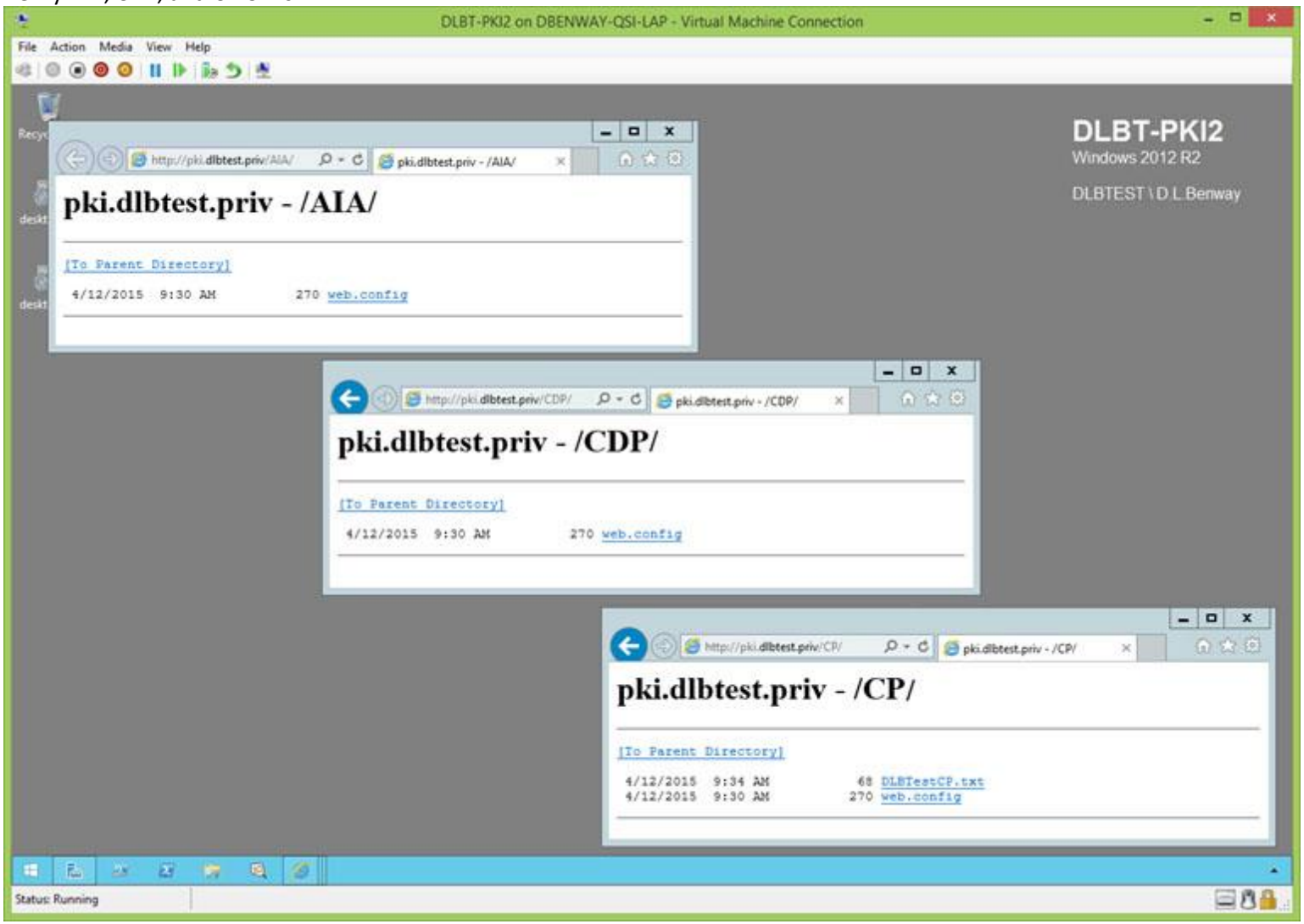
Write the CP (Certificate Policy) and save it in C:\InetPub\PKI\CP, and make its filename match that specified in the sub/policy/issuing CA's CAPolicy.inf.



Verify AIA, CDP, and CP URLs:

(jump to TOC)

Verify AIA, CDP, and CP URLs:



Root CA:

(jump to TOC)

This heading is just a TOC placeholder.

Root CA's CAPolicy.inf (Before CertUtil.exe):

(jump to TOC)

WARNING: This CAPolicy.inf file has a lot of important comments that need to be read and understood, or problems will arise.
Note: Because the CAPolicy.inf and Certutil.exe files in this document have been updated since initial publication, the values in this document's screenshots (such as registry settings, publication intervals, etc.) might not always reflect the values from these files.

To build the root CA, first write (in %SystemRoot%) the CAPolicy.inf file:

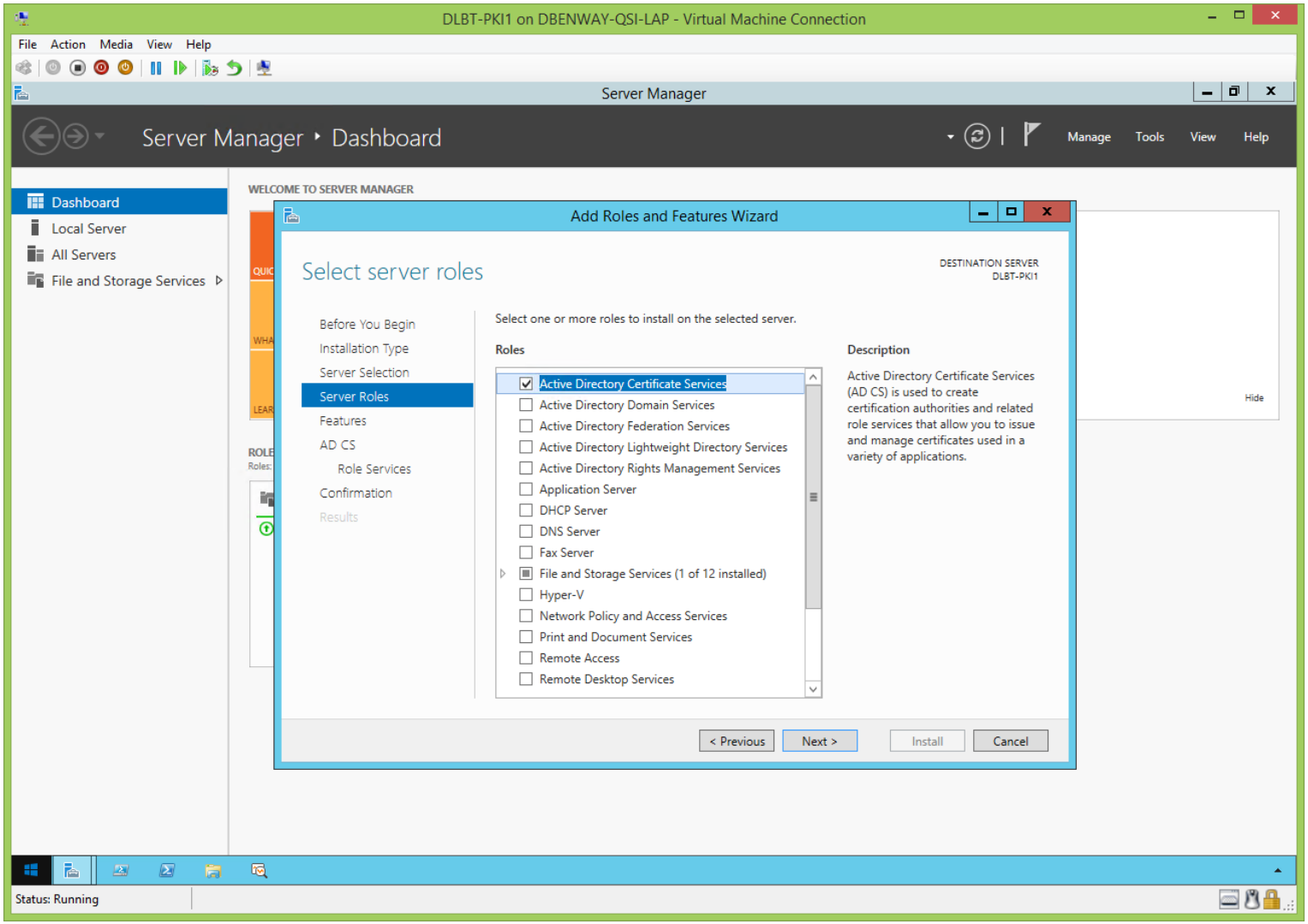
```
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; CAPolicy.inf Root
;
; CAPolicy.inf is used during ADCS installation of the local CA, and renewal of the local CA's certificate.
; Save it in %systemRoot% in ANSI format.
; Remember to never install a CA on a DC (it's a violation of best practice, but since this CA is offline that isn't even possible).
;-----------------------------------------------------------------------------------------------------------------------------------------------------------

;###########################################################################################################################################################
[Version]
Signature="$Windows NT$"

;###########################################################################################################################################################
[CertSrv_server]
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; This root CA's certificate will be self-signed, as is normal for a root CA.
; This root CA's certificate has a key length, and a certificate validity period which is specified during its local ADCS installation GUI wizard.
; The key length and validity period of the certificates this root CA issues is specified in its registry (standalone CAs configure validity periods for the
; certificates they issue in their registry, enterprise CAs do it in the enterprise templates (and if not there then it defaults to their registry)).
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; These renewal settings affect renewal of this root CA's certificate (because there is no enterprise template which defines them and standalone CAs don't
; even use enterprise templates, and because the local ADCS installation GUI would have already been run at the time of renewal).
; During renewal these settings will default to match the existing certificate. They have been explicitly set here for completeness and clarity.
; Key length 2048 is chosen for compatibility.
; The lowest certificates should have up to 5 years, so sub/policy/issuing CA's certificate is 10, so root CA's certificate is 20.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
RenewalKeyLength=2048
RenewalValidityPeriodUnits=20
RenewalValidityPeriod=years

;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; We want to support Windows OSs earlier than Vista, as well as Apple, Cisco, Java, etc., so disable alternate signatures for the certificates this
; root CA issues.
; Note: 'Discrete' has been deprecated and replaced by 'Alternate'.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
AlternateSignatureAlgorithm=0

;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; Do not load default certificate templates onto this root CA from the AD.
; This setting does not apply to stand-alone root CAs, much less stand-alone offline root CAs, and is just included for completeness and clarity.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
LoadDefaultTemplates=0

;###########################################################################################################################################################
[CRLDistributionPoint]
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; These settings cause this root CA's certificate to contain no CDP information, which is current best practice for a root CA's certificate (the root CA
; certificate is normally not revocation checked).
```

```
; Windows Server 2003 and newer by default do not put CDP information into a root CA's certificate, so this is explicitly set here for completeness
; and clarity.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
empty=TRUE

;###########################################################################################################################################################
[AuthorityInformationAccess]
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; These settings cause this root CA's certificate to contain no AIA information, which is current best practice for a root CA's certificate (there is no
; higher CA whose certificate and signature would be checked).
; Windows Server 2003 and newer by default do not put AIA information into a root CA's certificate, so this is explicitly set here for completeness
; and clarity.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
empty=TRUE

;###########################################################################################################################################################
[BasicConstraintsExtension]
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; The subject type in this root CA's certificate is 'CA'.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
Subject Type=CA

;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; PathLength should be set on the policy CA, not the root CA, to provide the greatest future flexibility for change.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
PathLength=none

;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; This section may not be skipped.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
Critical=true
```

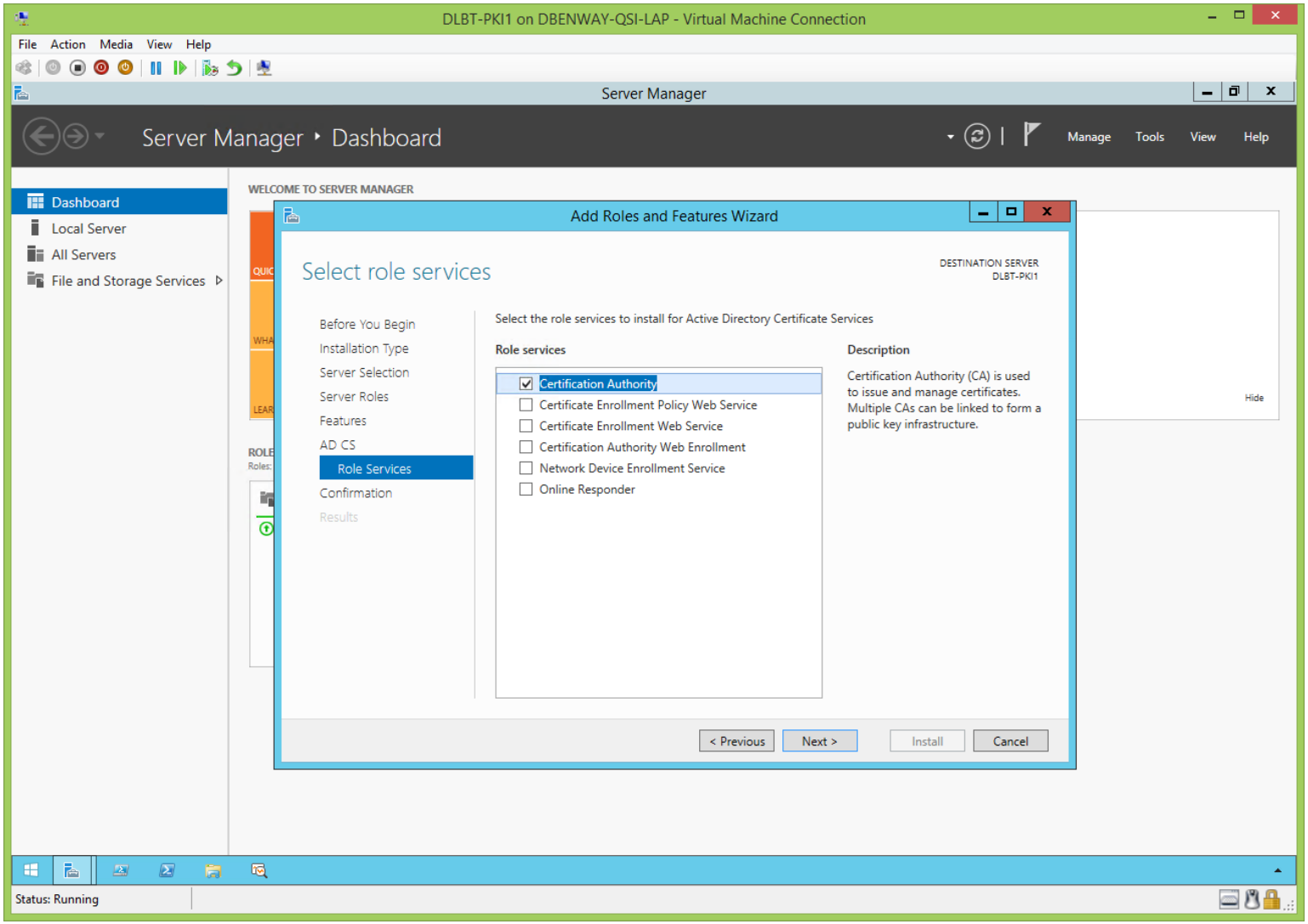
Root CA's ADCS Installation Wizard (Before CertUtil.exe):

(jump to TOC)

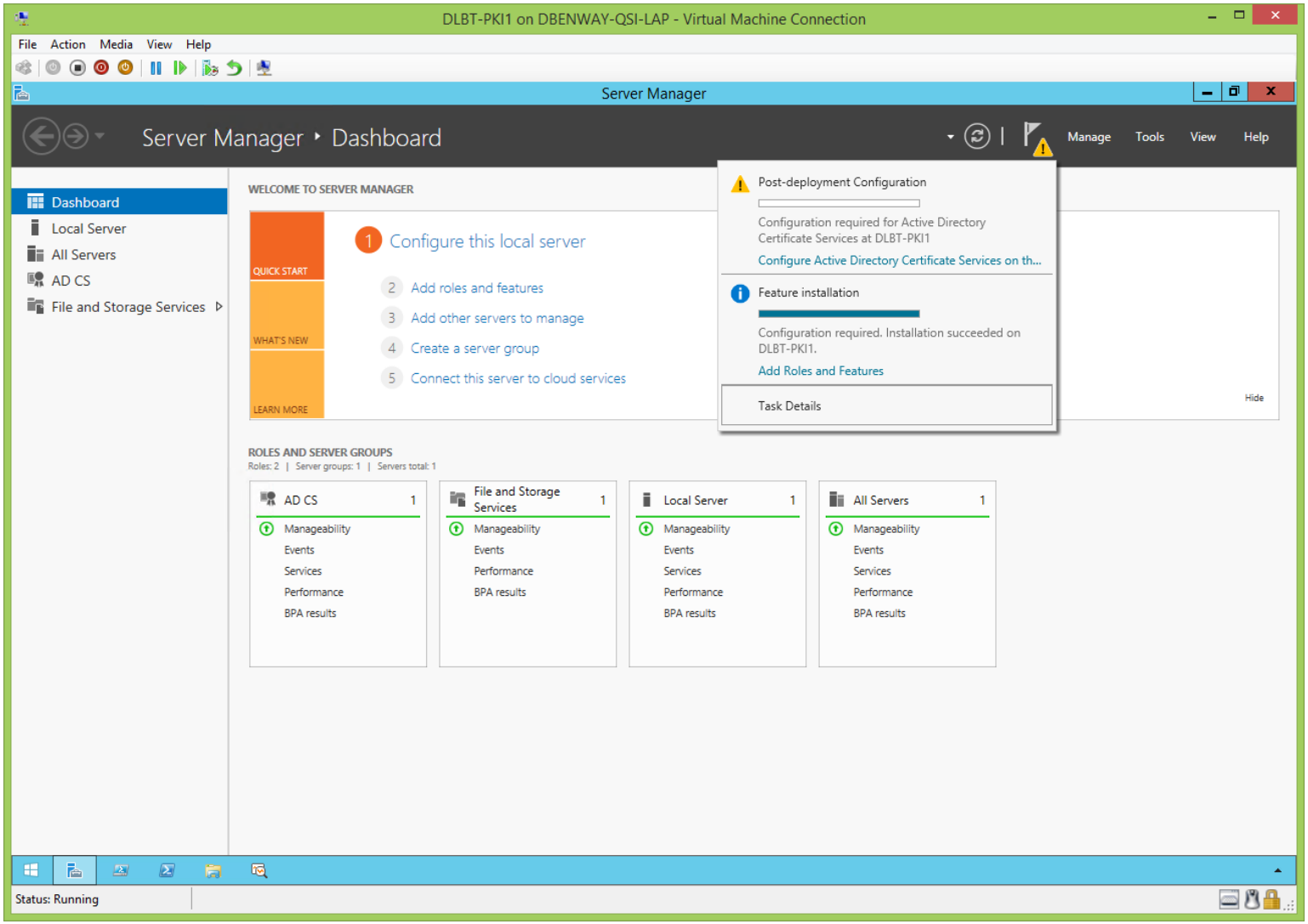
Install ADCS onto a workgroup-member, non-network-attached server, which will become the root CA:



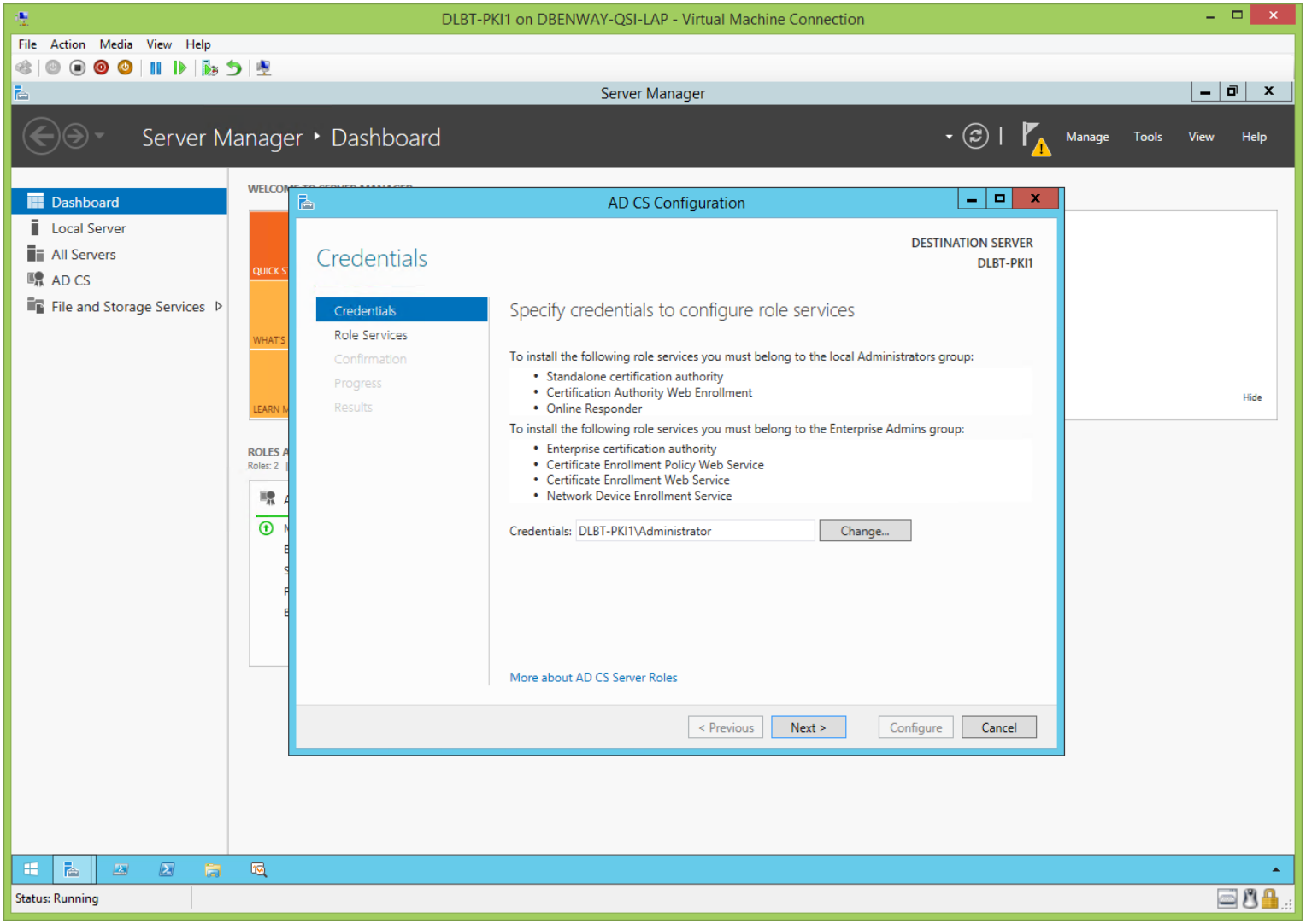
Being that this is the root CA, we only need it to be a Certification Authority:



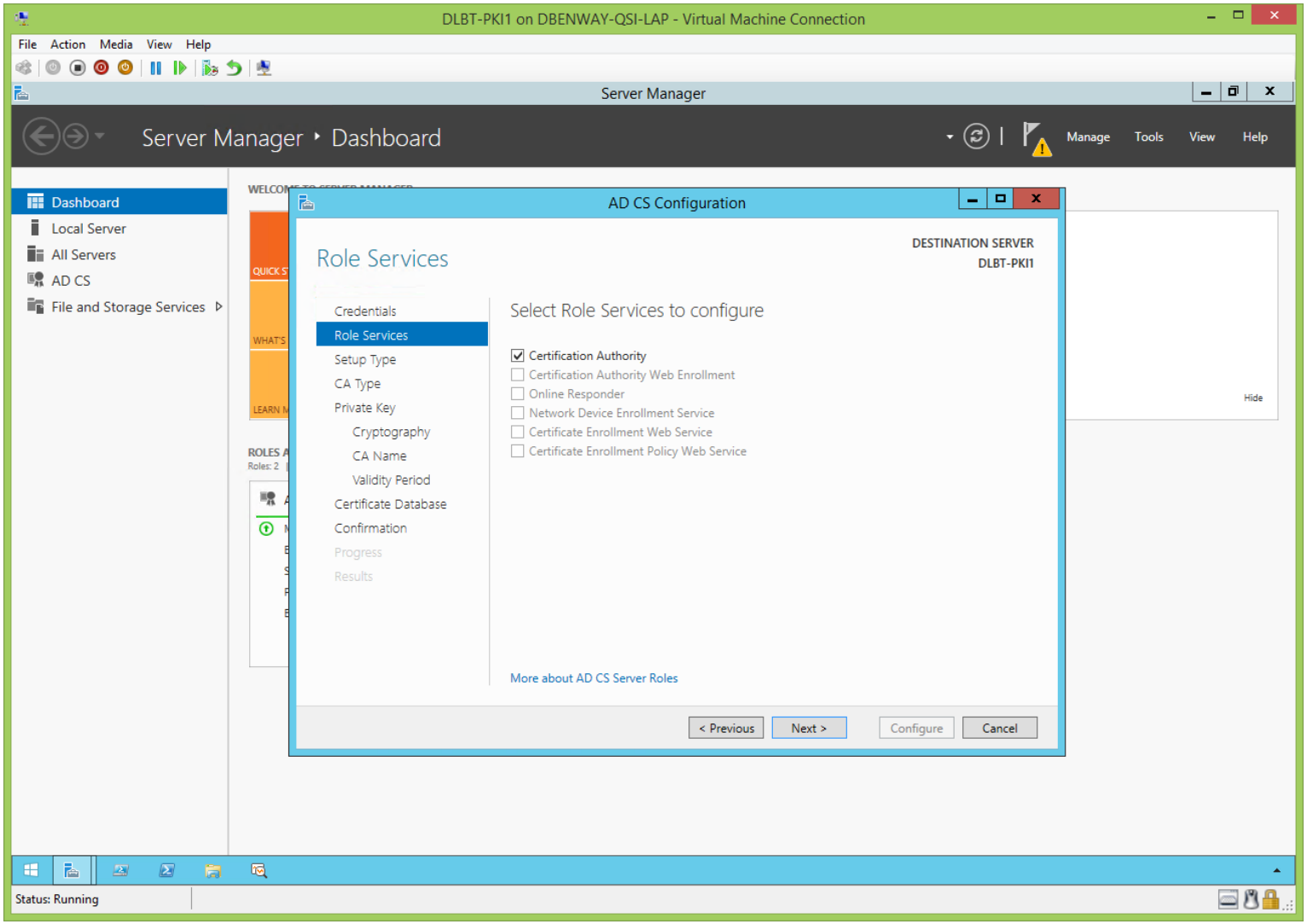
After installation of ADCS, we need to configure the root CA:



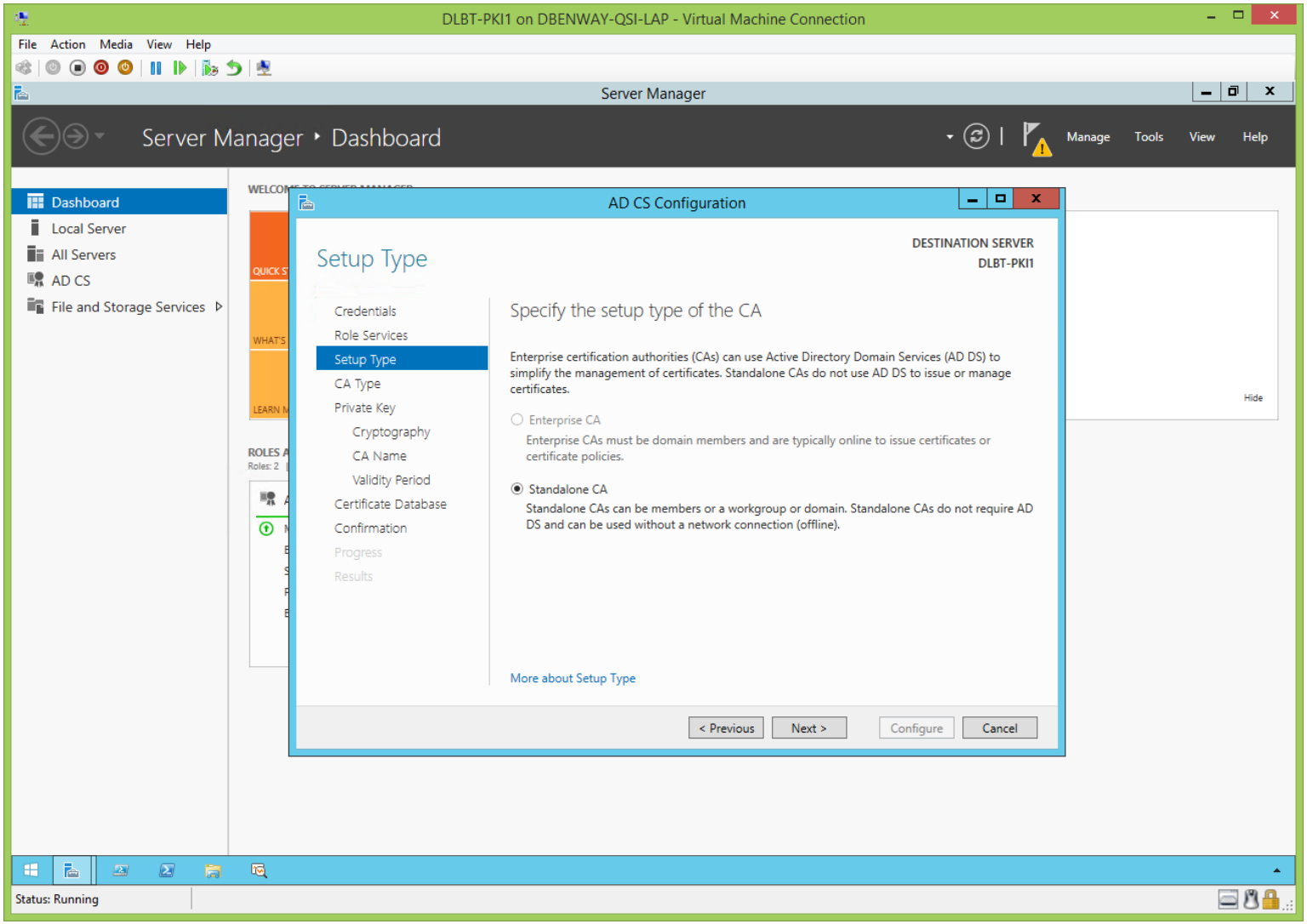
We'll do this configuration using the local Administrator account (this is a workgroup-member, non-network-attached server):



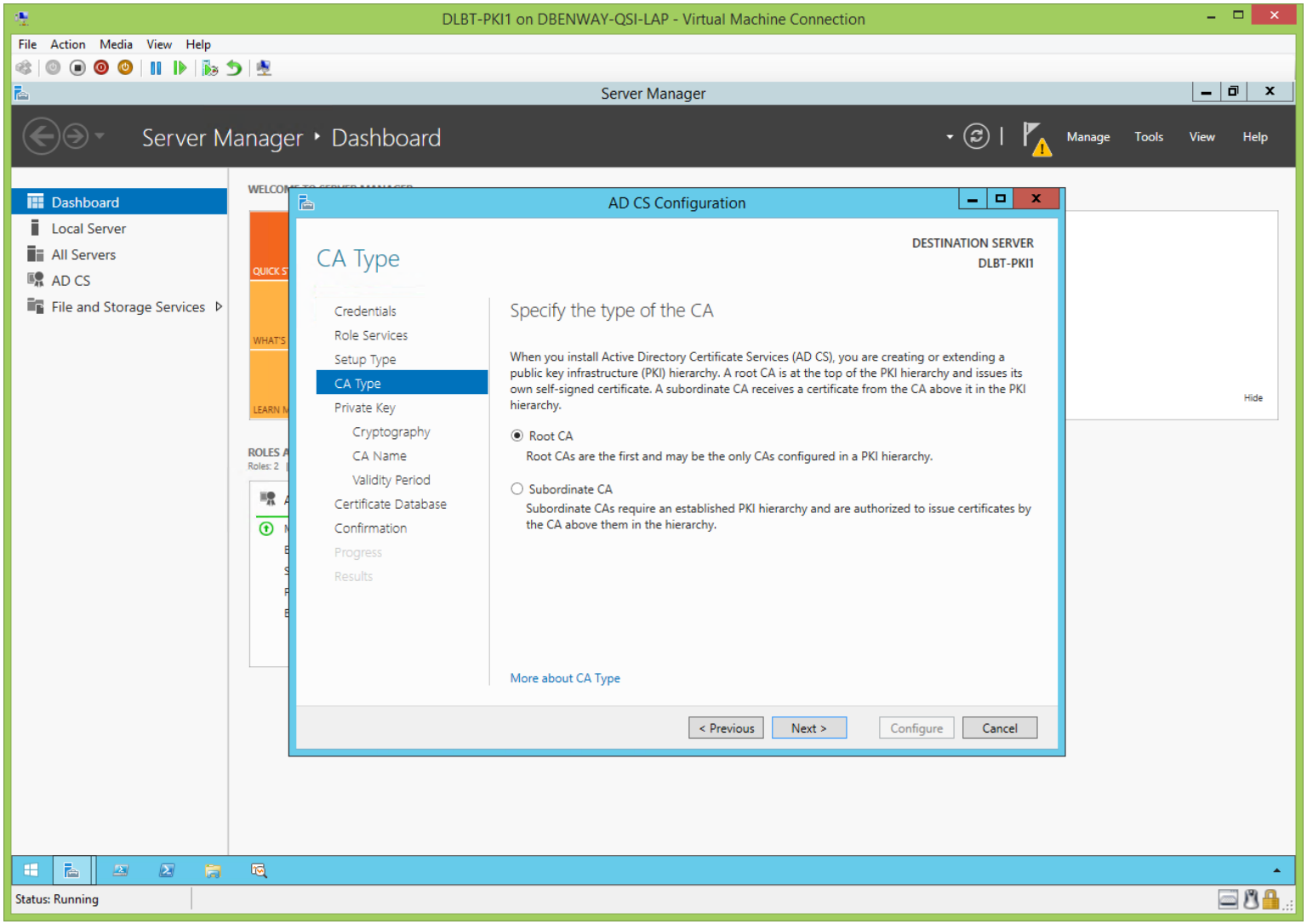
As the root CA this is just a Certification Authority:



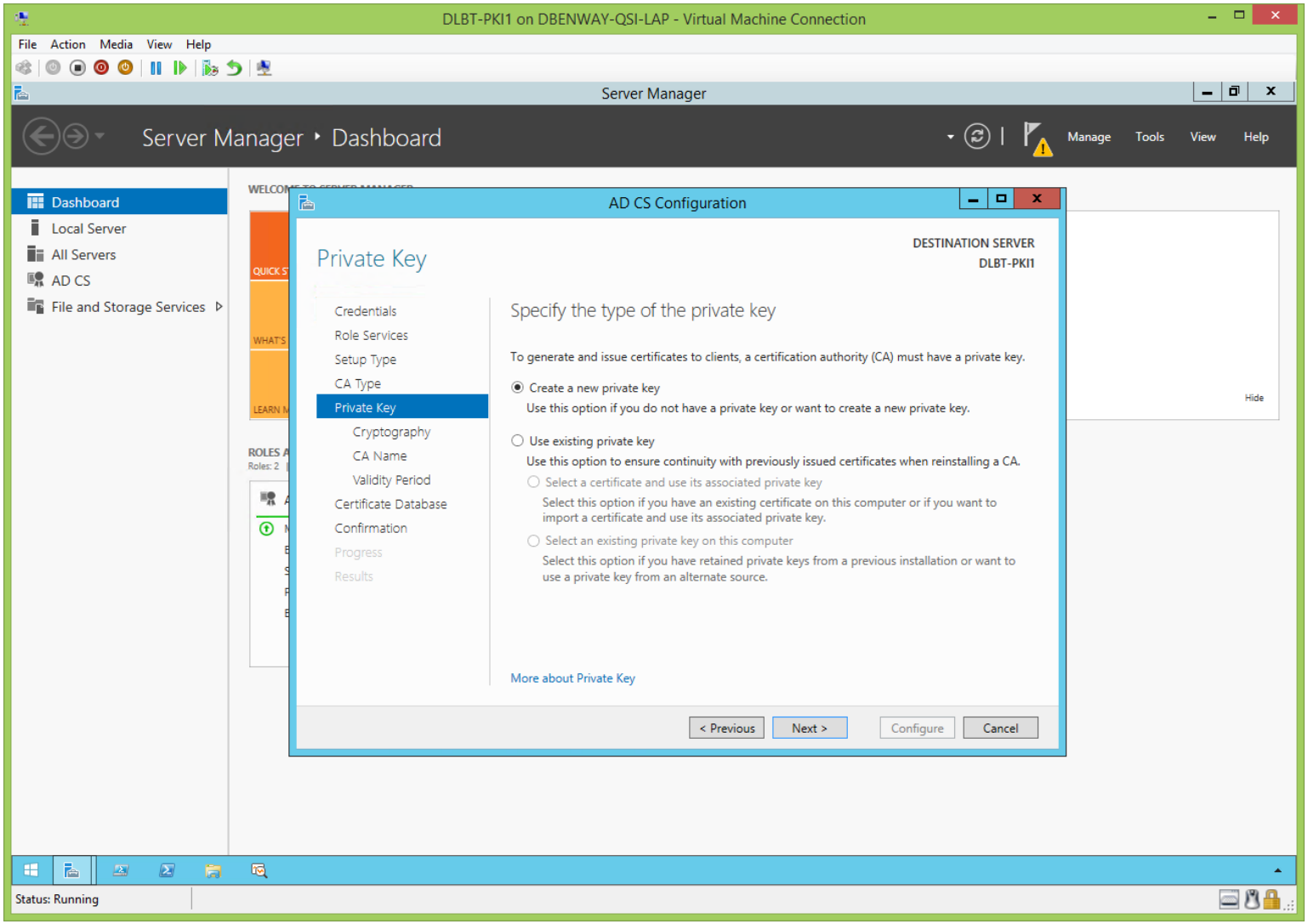
This is a workgroup-member, non-network-attached server, so of course it's a standalone CA:



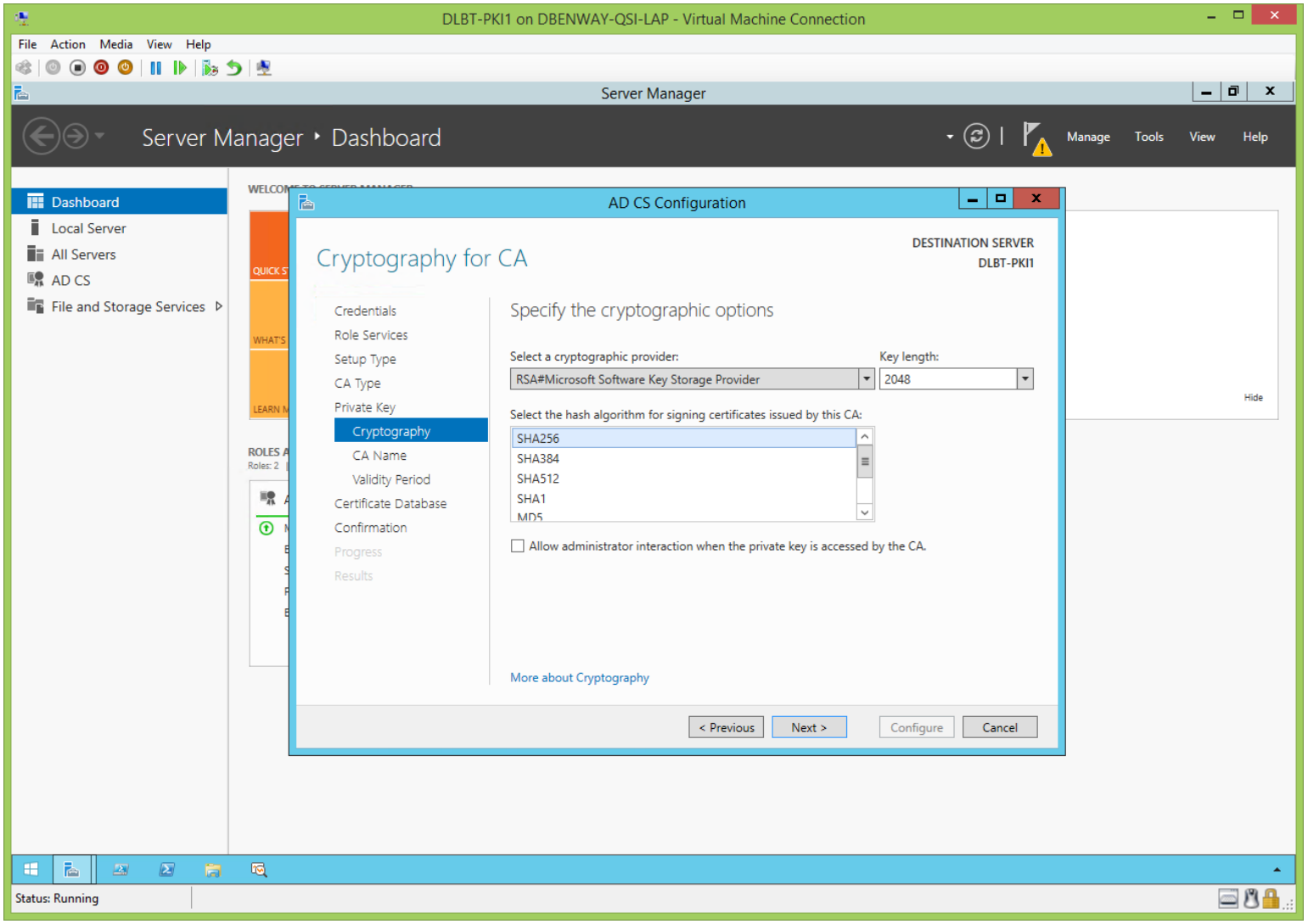
This is the root CA:



This is a new PKI, so we'll create a new private key for the root CA:

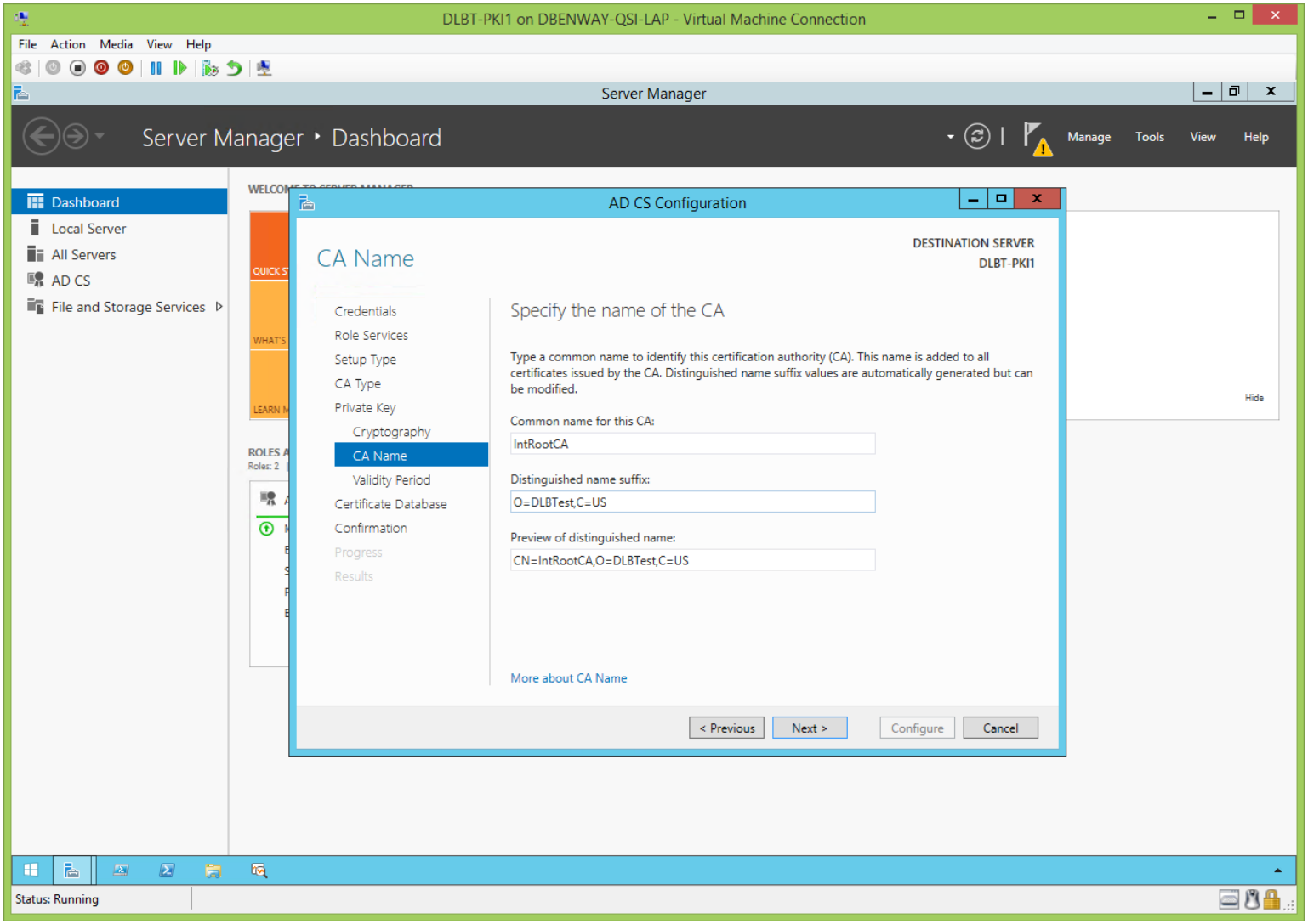


- Microsoft's software Key Storage Provider (MS KSP) will be the Cryptographic Storage Provider (CSP) used by this root CA.
- Key length 2048 is just for this root CA's certificate. 2048 was chosen because it's highly compatible. Remember that a root CA's certificate is self-signed.
- SHA256 is the hash algorithm used by this root CA (SHA1 is no longer secure, so don't use it).

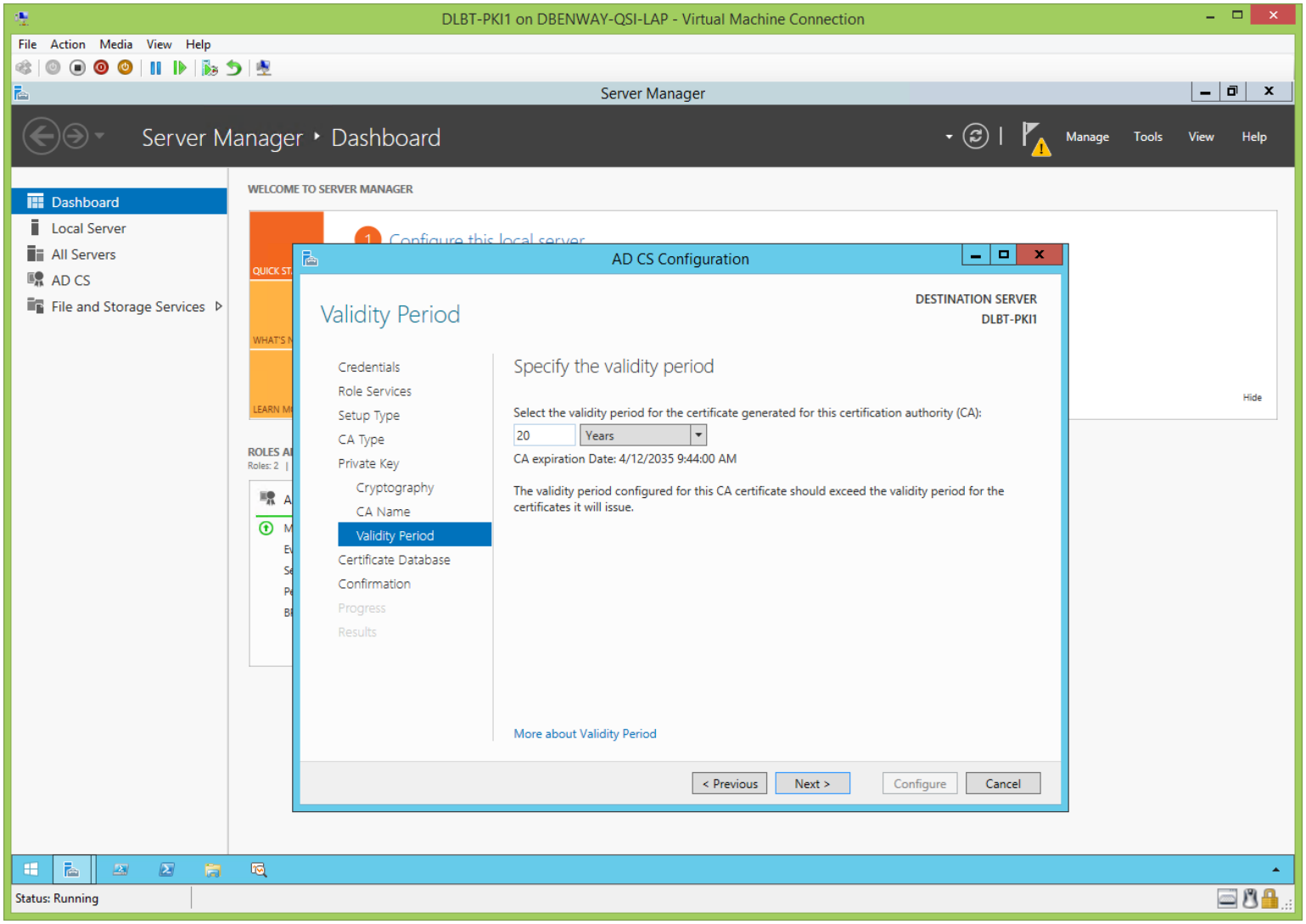


Give the CA a meaningful name (not identical to its hostname) like IntRootCA. I like to keep the name to 15 or fewer characters in case there's a NetBIOS compatibility issue.

The distinguished name suffix is usually the system's AD distinguished name minus its hostname, but this is a standalone server so let's do this:

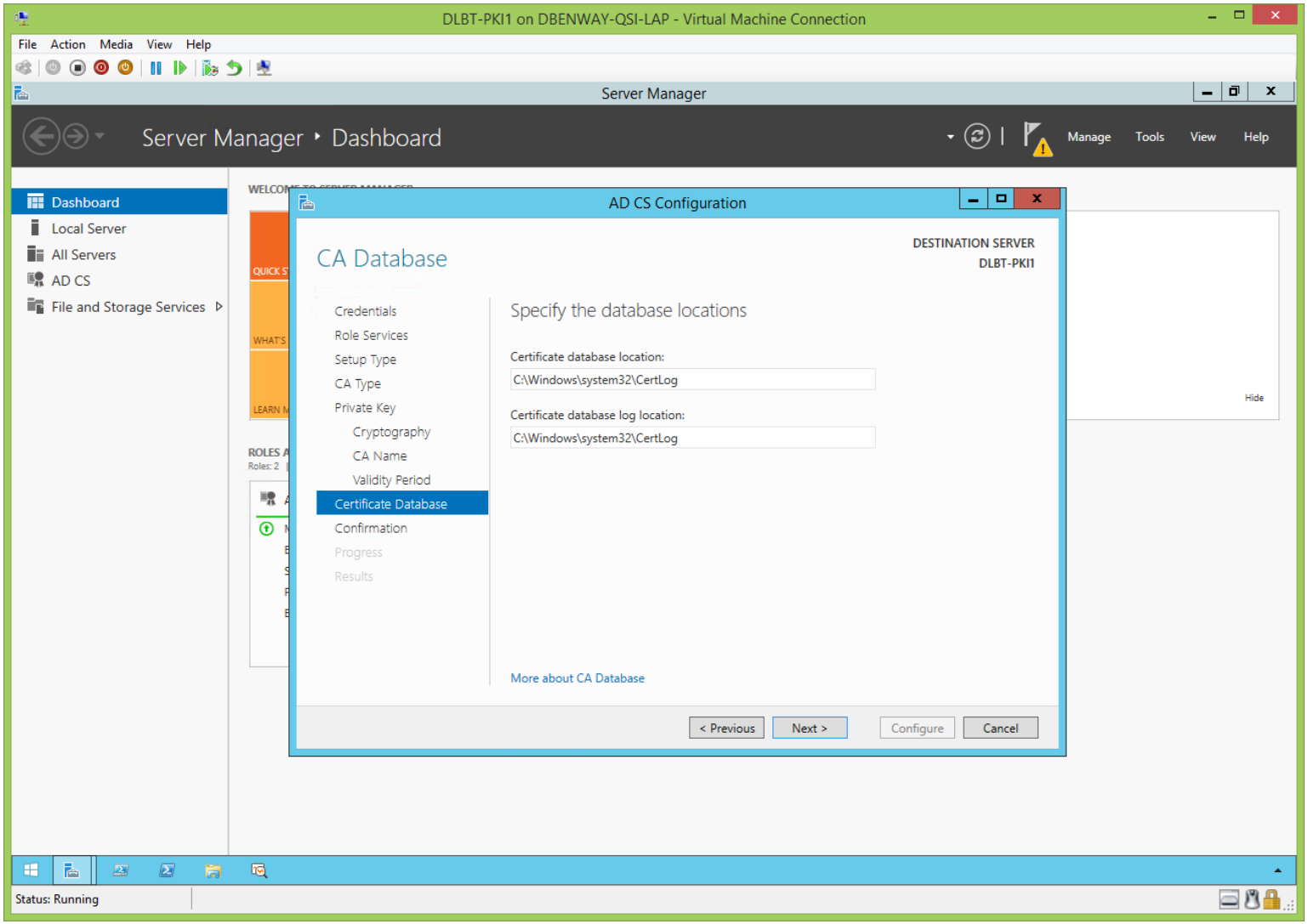


Set the validity period for the root CA's certificate (the root certificate):

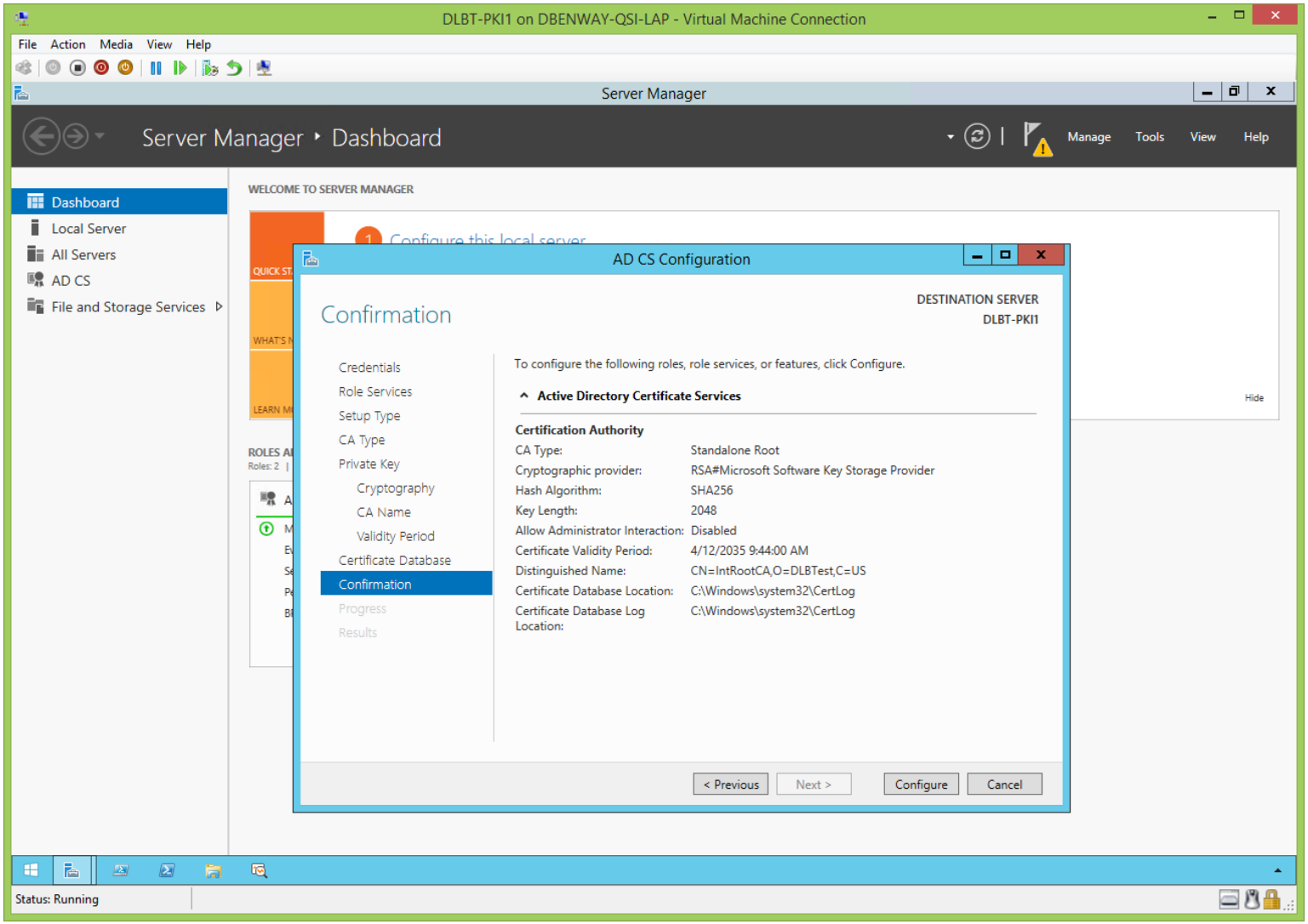


For a 2-tier PKI, the rule of thumb is: if the issuing CAs need to issue certificates with a 5 year validity period, then the sub/policy/issuing CA's certificate should have double that, a 10 year validity period, and the root CA's certificate should have double that, a 20 year validity period (Komar p.88).

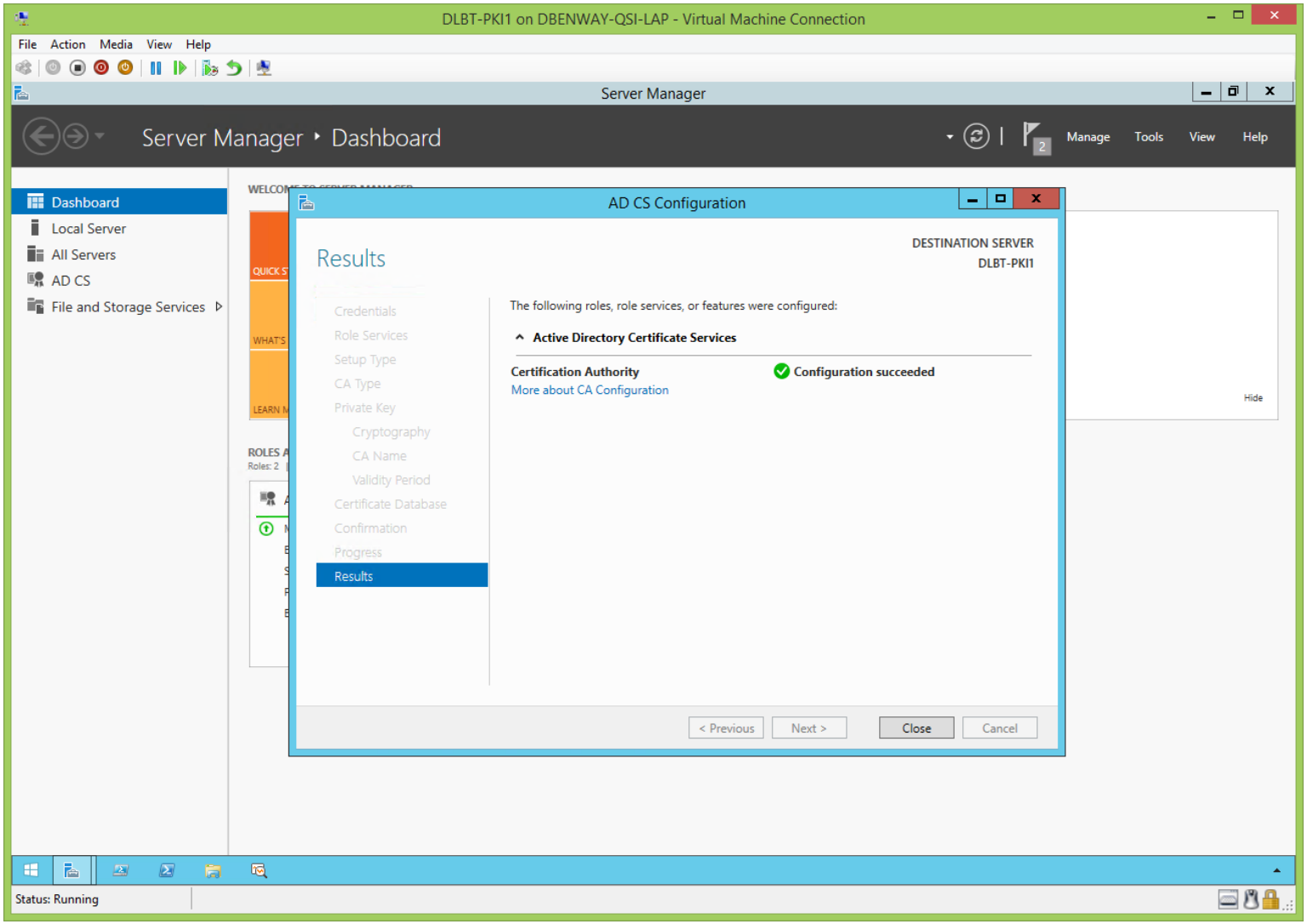
Set the desired location for the local ADCS database and logs:



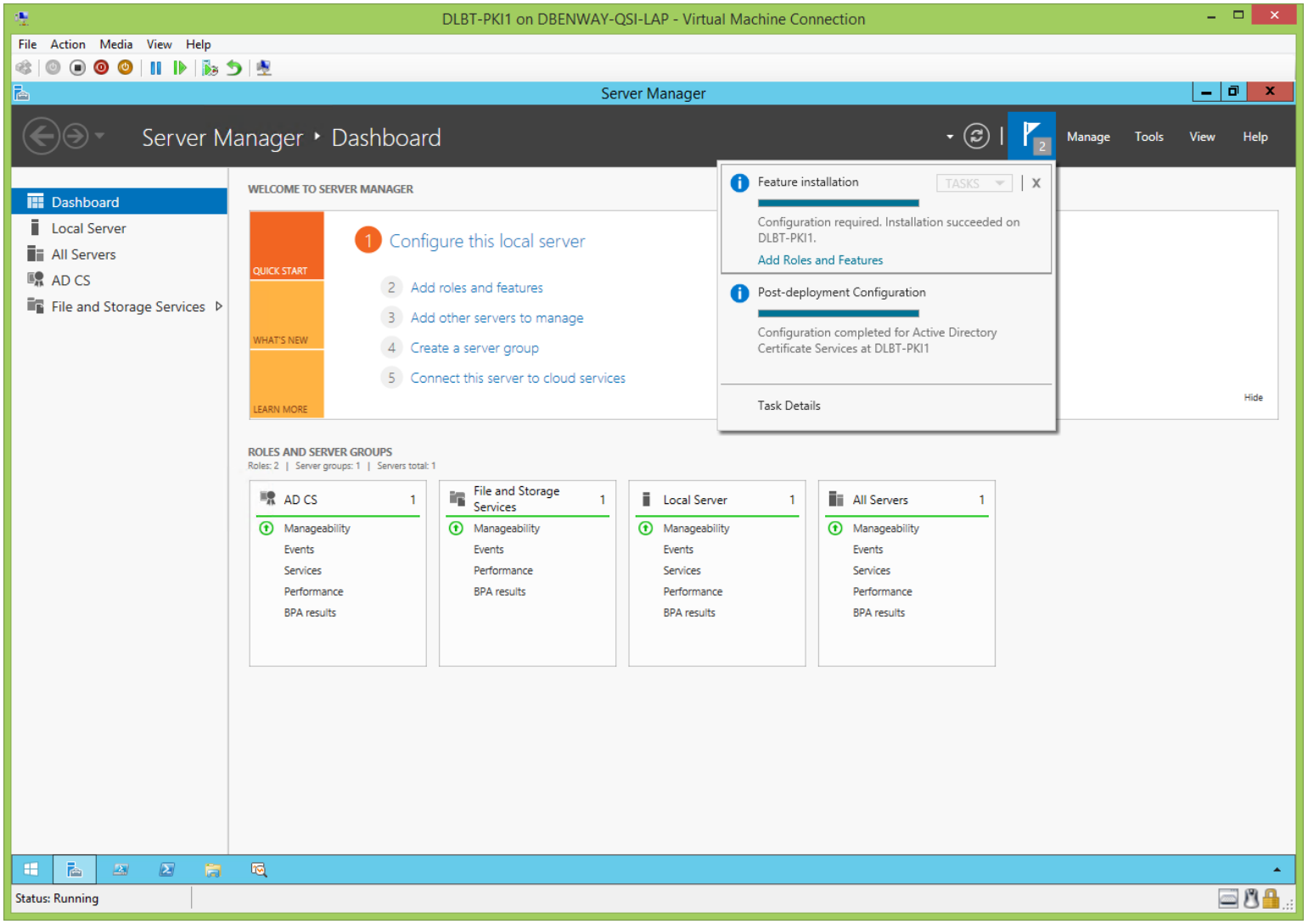
Review the configuration:



Configuration was successful:



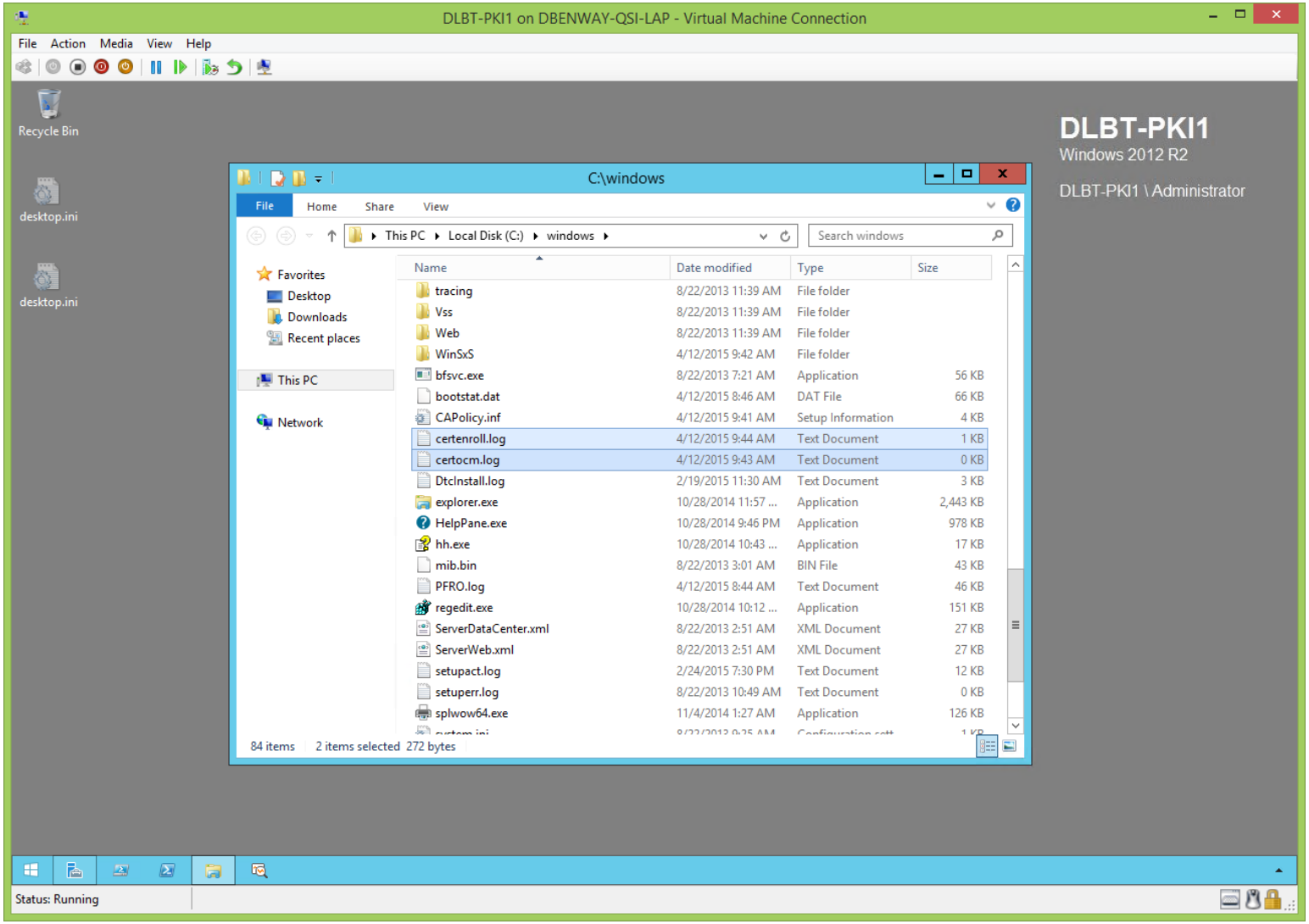
ADCS has been installed and configured:



Root CA's Logs (Before CertUtil.exe):

(jump to TOC)

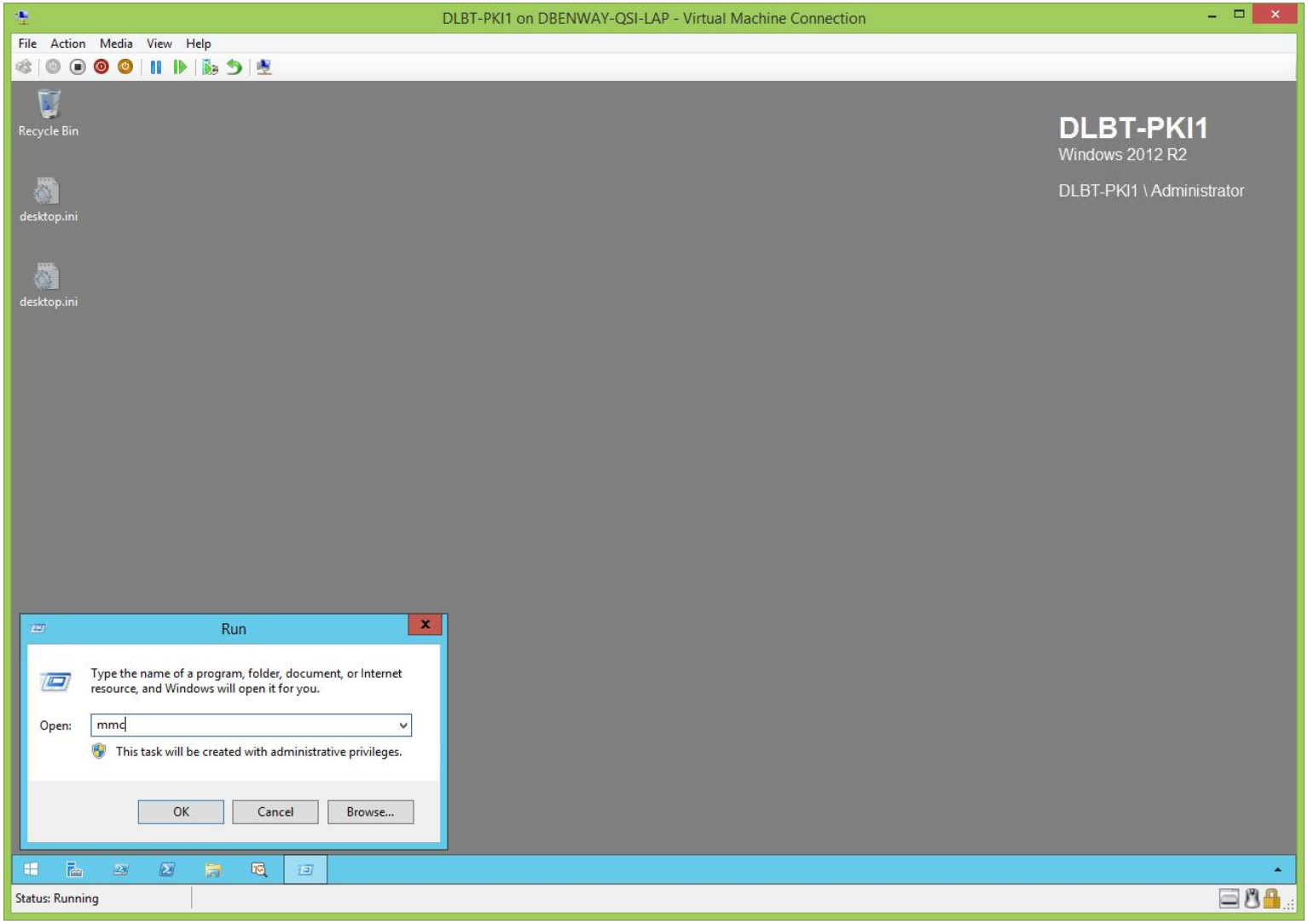
You can view the log files, but they so carelessly use the words 'error' and 'fail' that I found them to be of limited value:



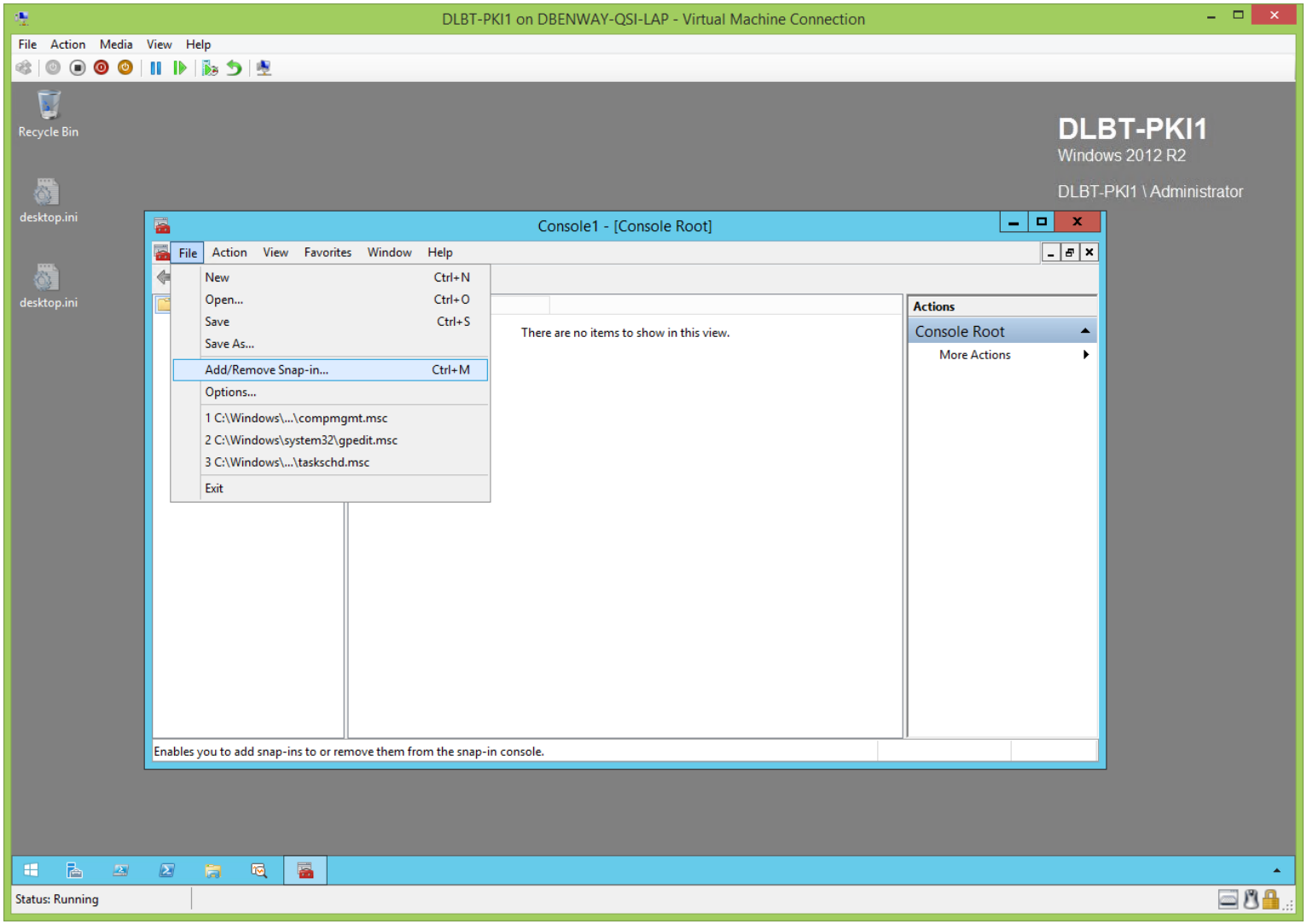
Root CA's PKI MMC (Before CertUtil.exe):

(jump to TOC)

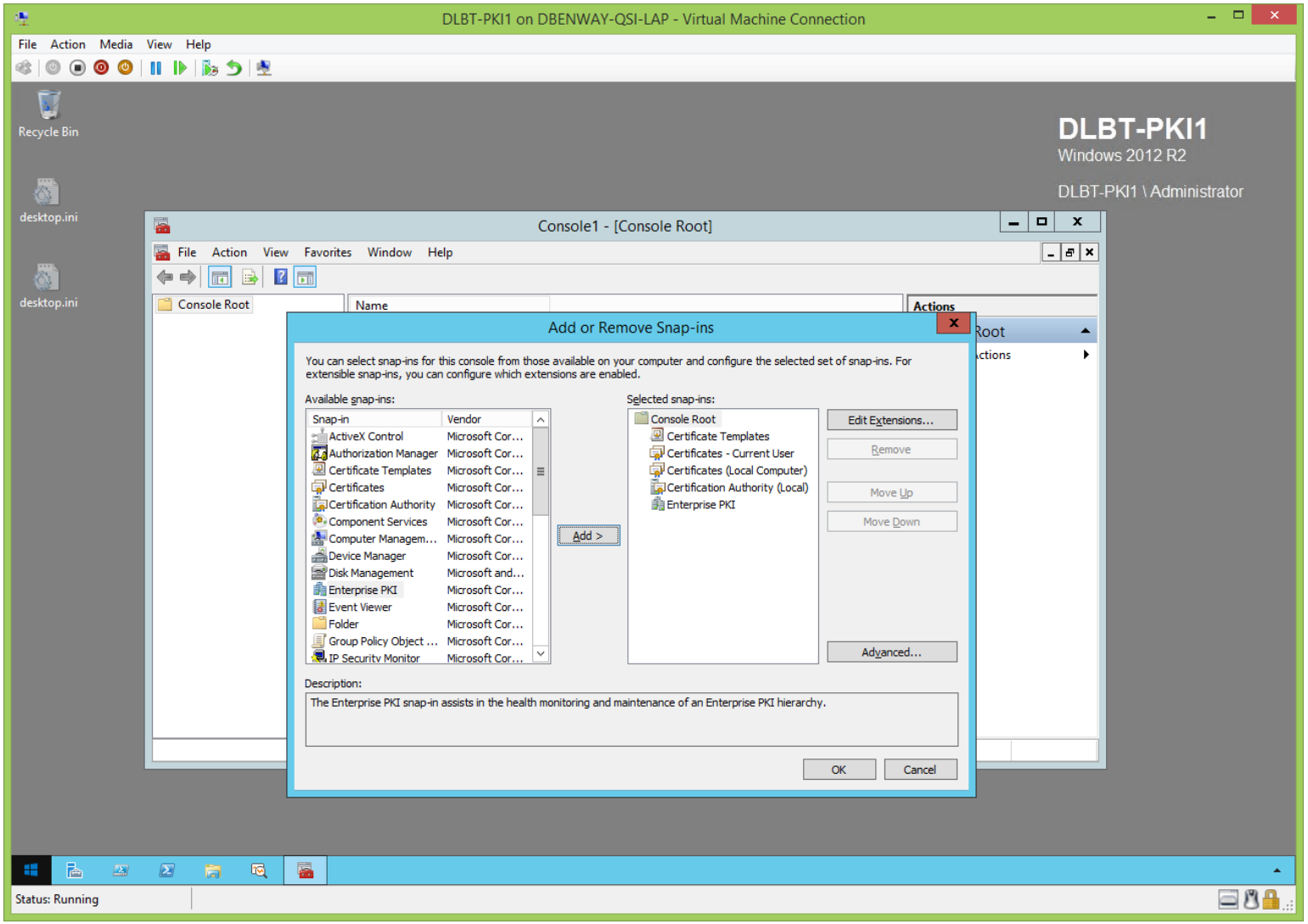
Now let's set up the PKI MMC on the root CA:



Add the snap-ins:

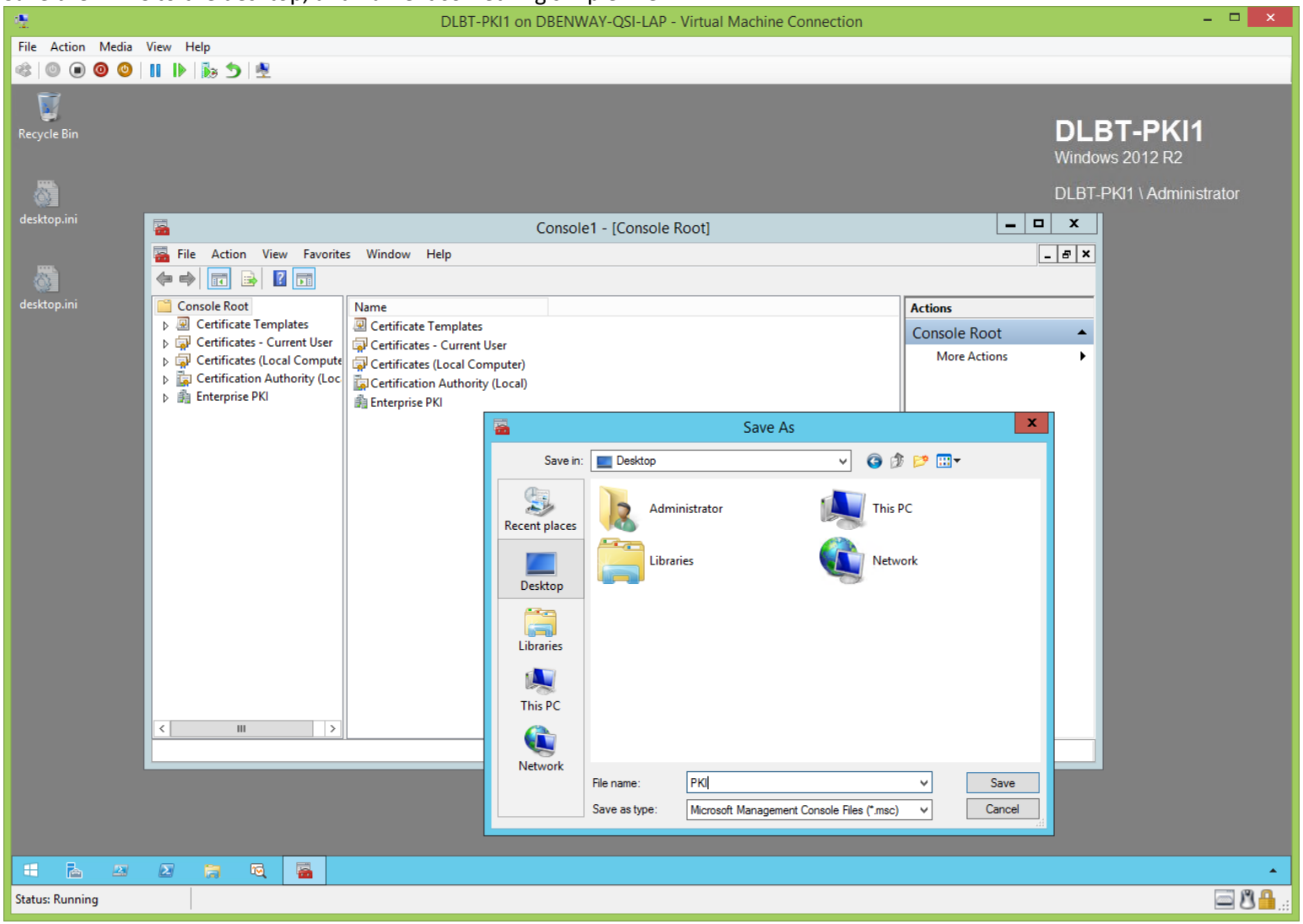


Add Certificate Templates, Certificates (for Current User and Local Computer), Certification Authority, and Enterprise PKI:



This is a standalone CA so we don't need to add 'Certificate Templates' or 'Enterprise PKI' to the snap-in, but it's just a good habit to get into.

Save the MMC to the desktop, and name it something simple like 'PKI':



Root CA's Enterprise PKI Snap-In (Before CertUtil.exe):

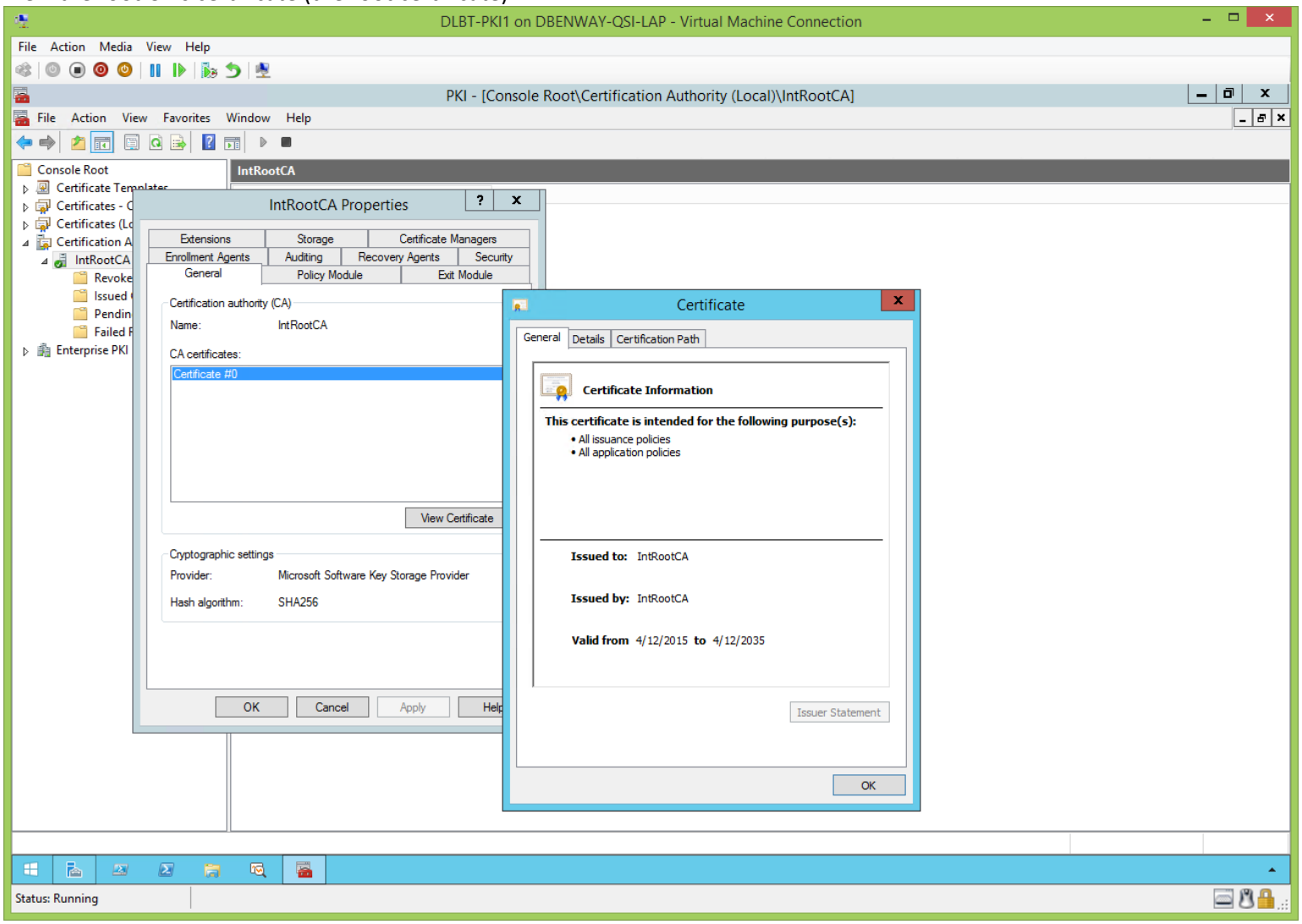
(jump to TOC)

The root CA can't use this because it's not an Enterprise CA, nor can it see templates.

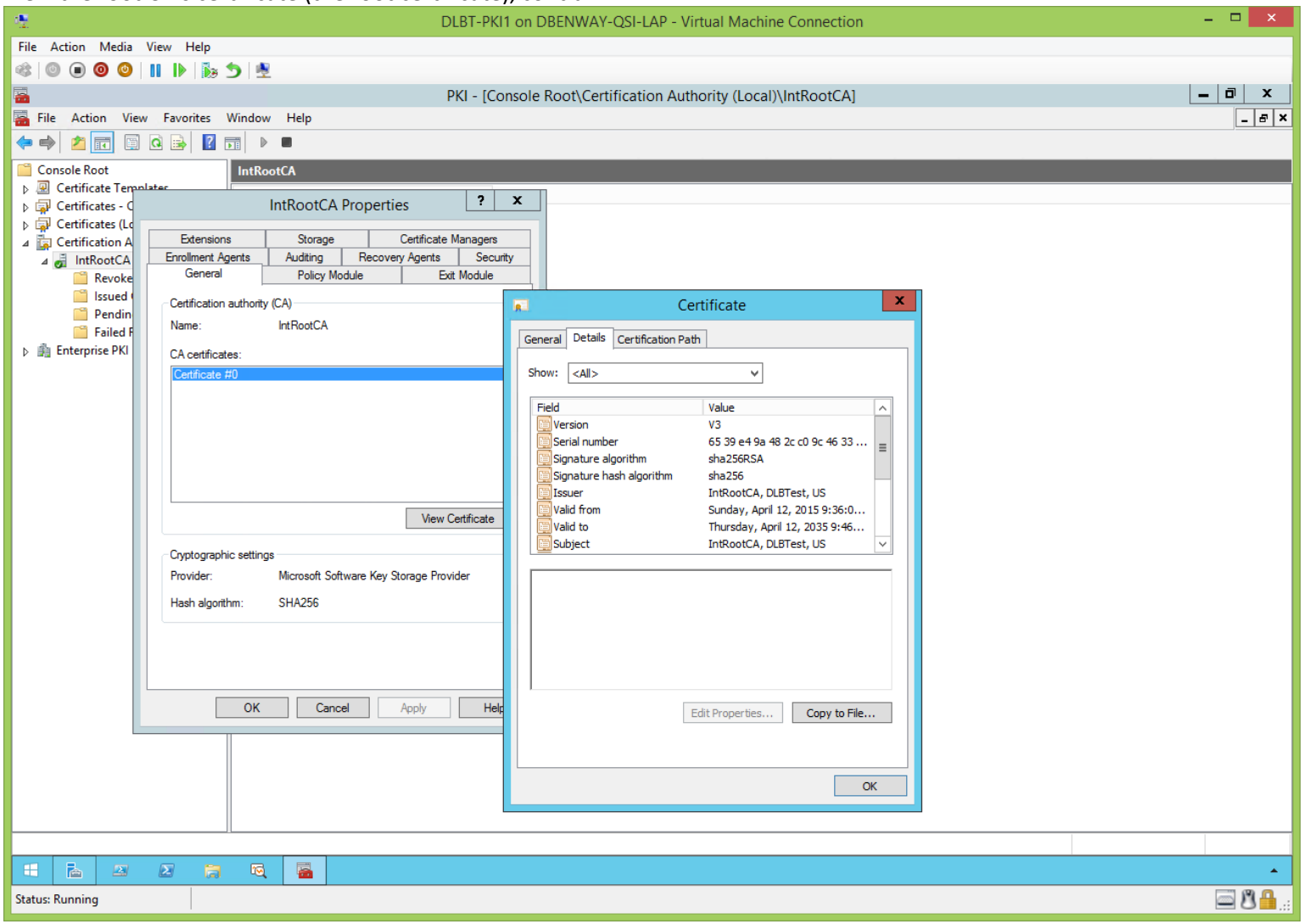
Root CA's Certificate (Before CertUtil.exe):

(jump to TOC)

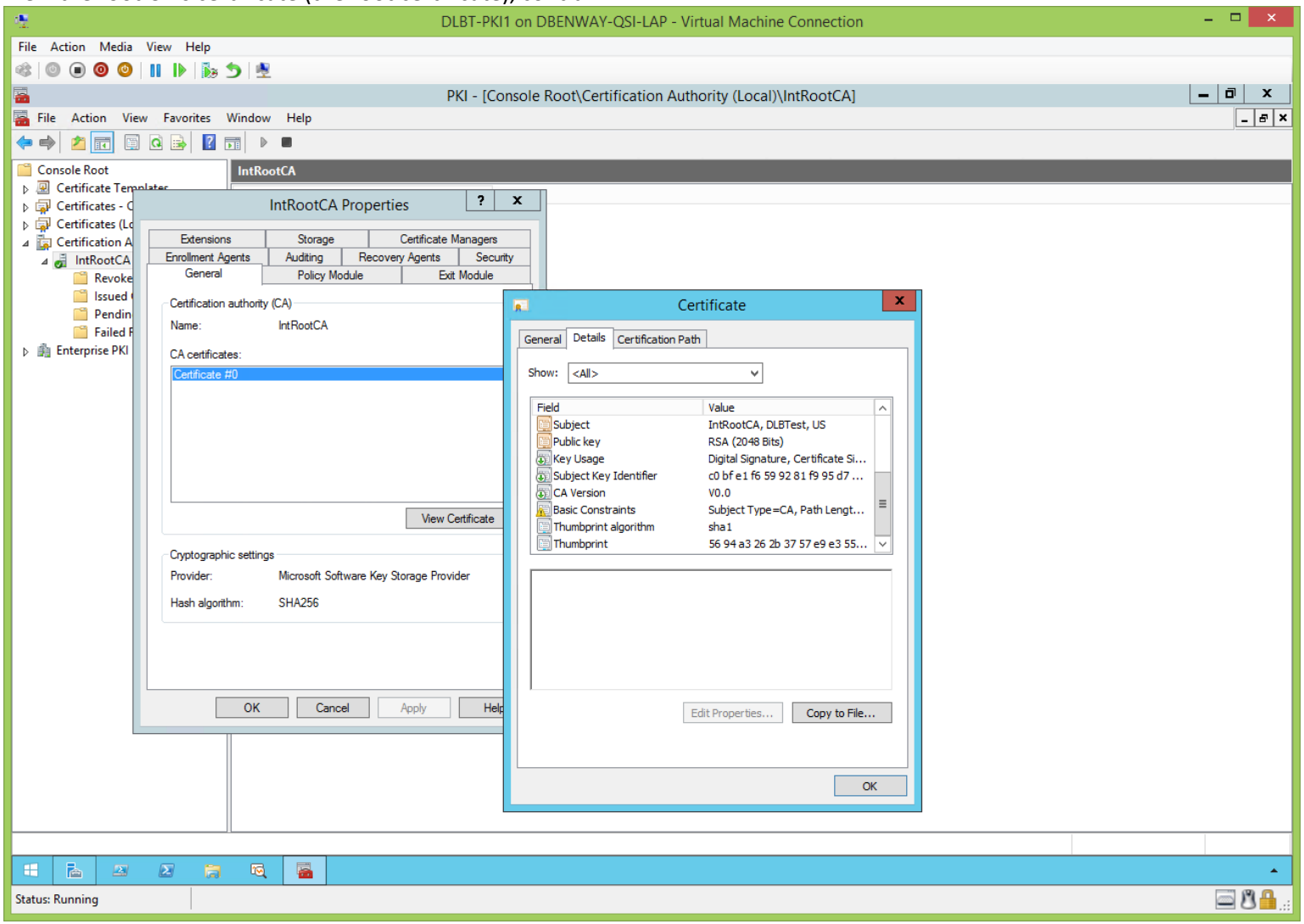
View the root CA's certificate (the root certificate):



View the root CA's certificate (the root certificate), cont'd:

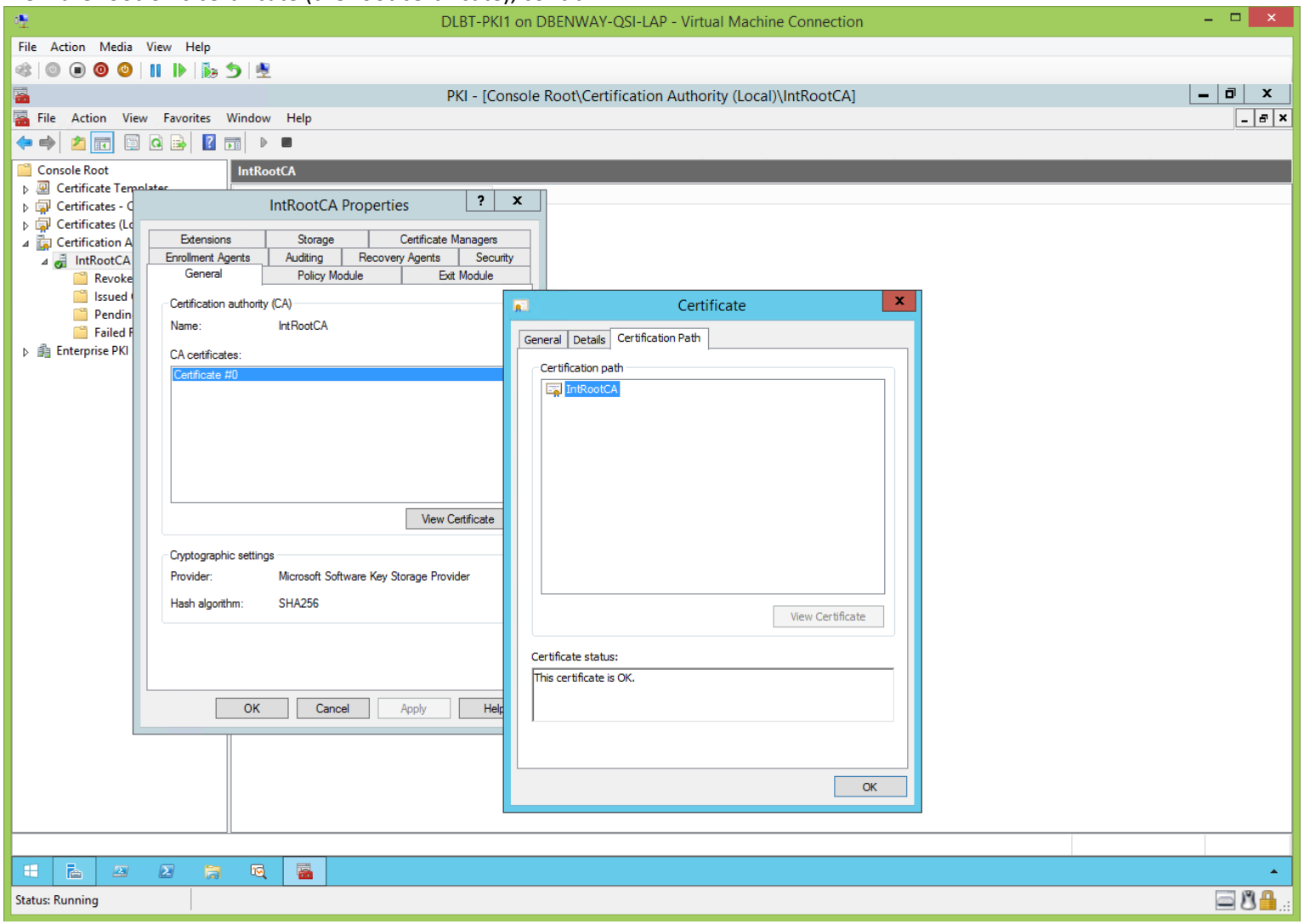


View the root CA's certificate (the root certificate), cont'd:



The yellow exclamation point means the Basic Constraints are critical, as specified in the CAPolicy.inf.

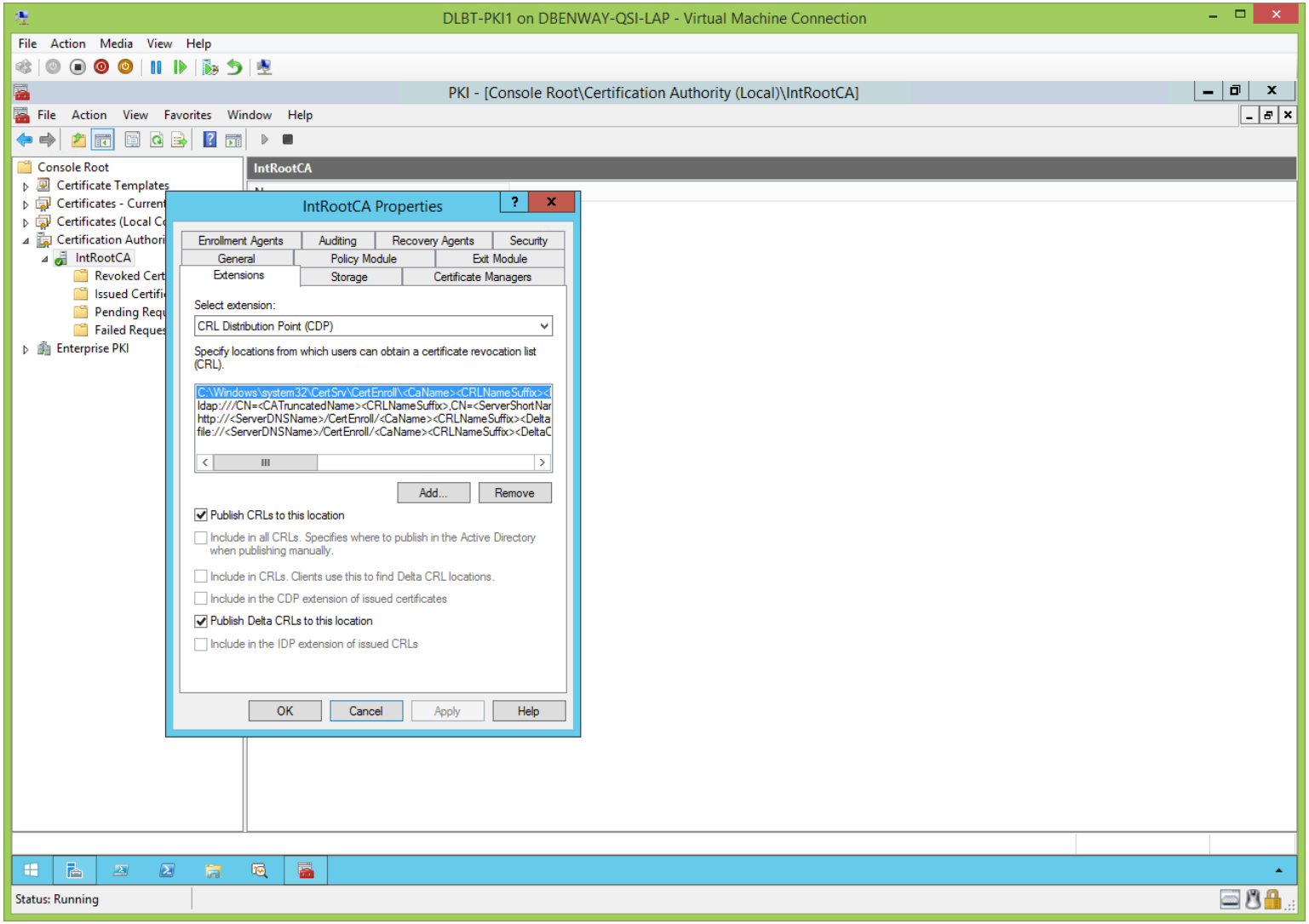
View the root CA's certificate (the root certificate), cont'd:



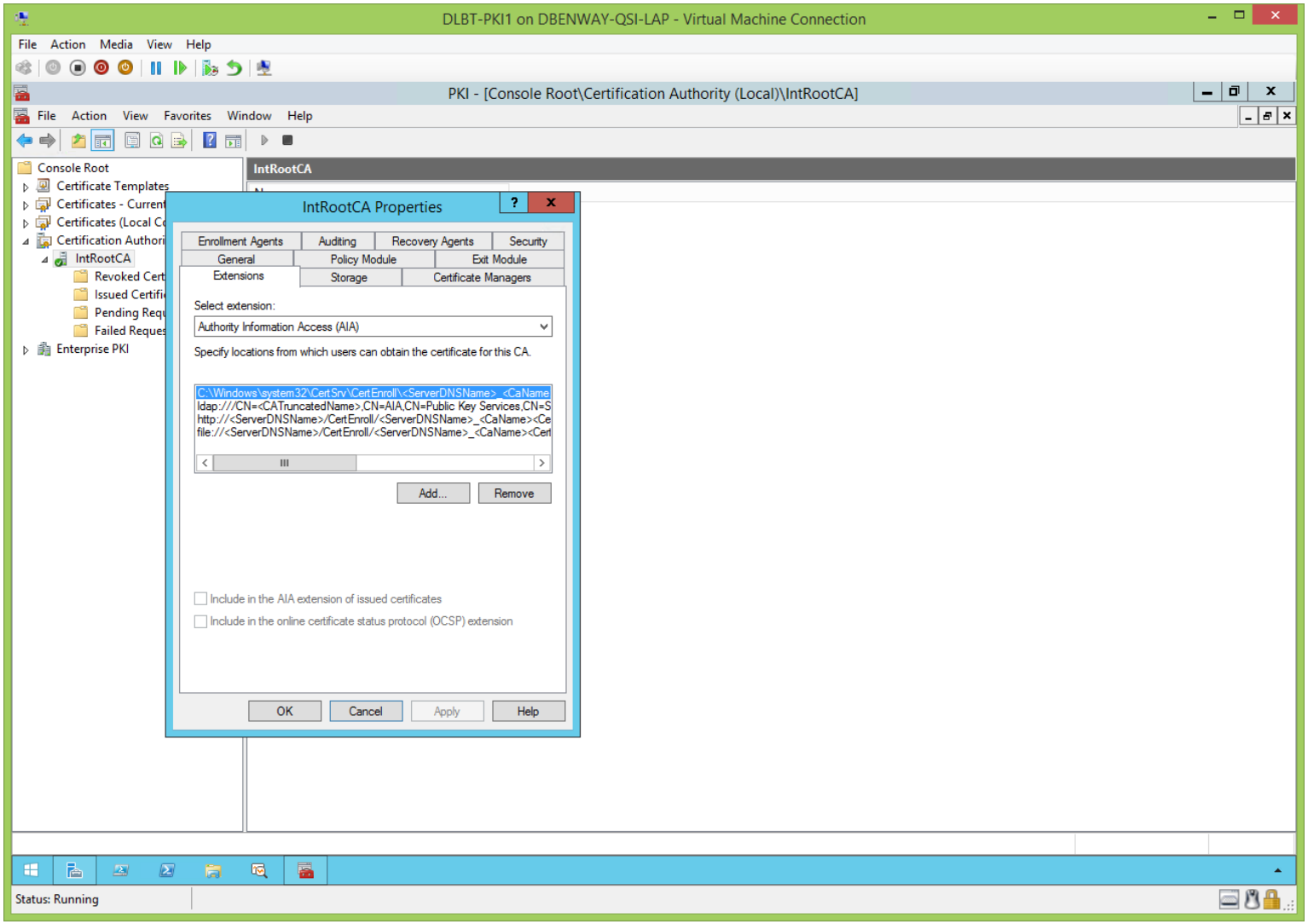
Root CA's Extensions (Before CertUtil.exe):

(jump to TOC)

These extensions are properties of the root CA, and we'll change these later with CertUtil.exe:



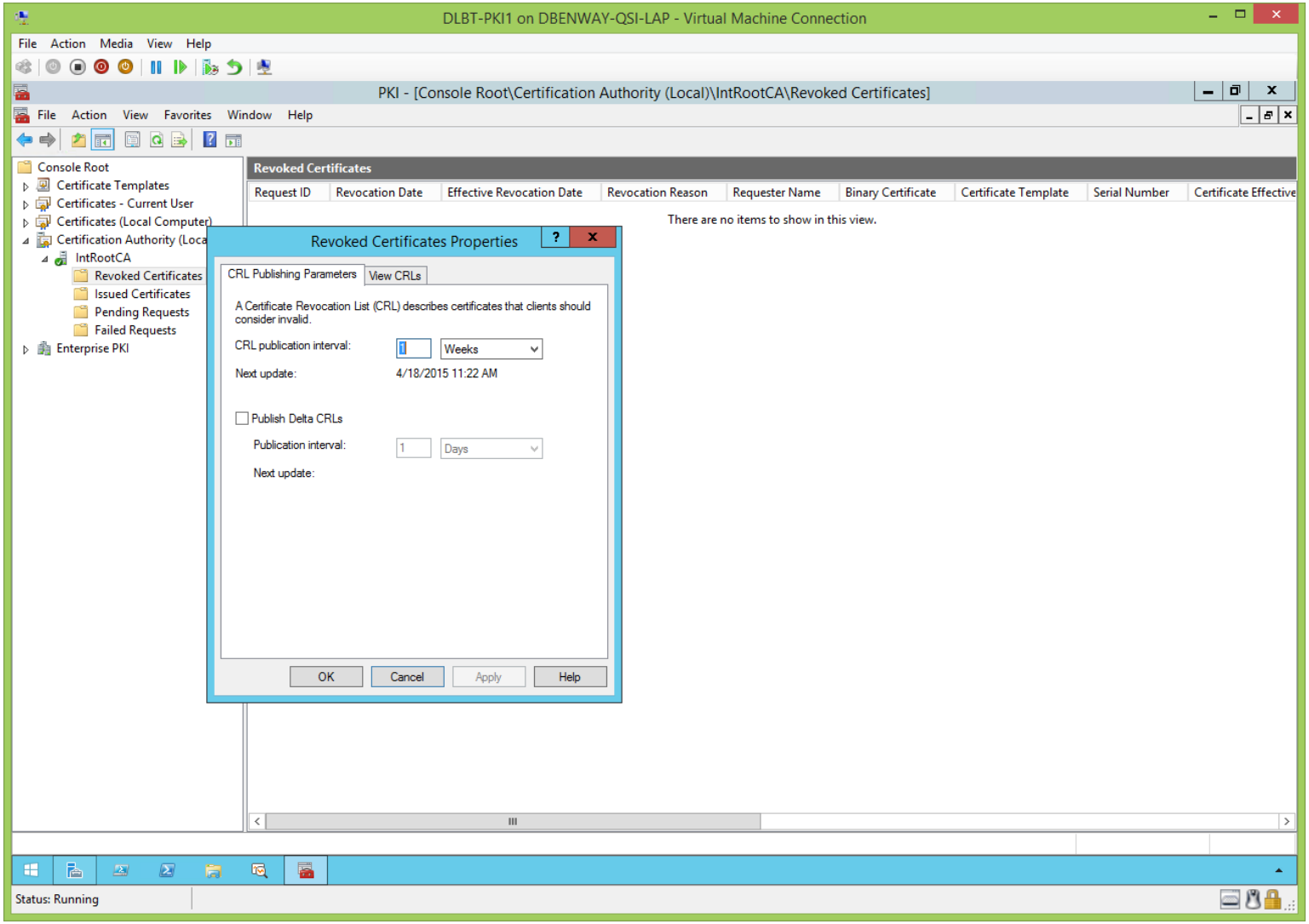
View CA extensions, cont'd:



Root CA's CRLs (Before CertUtil.exe):

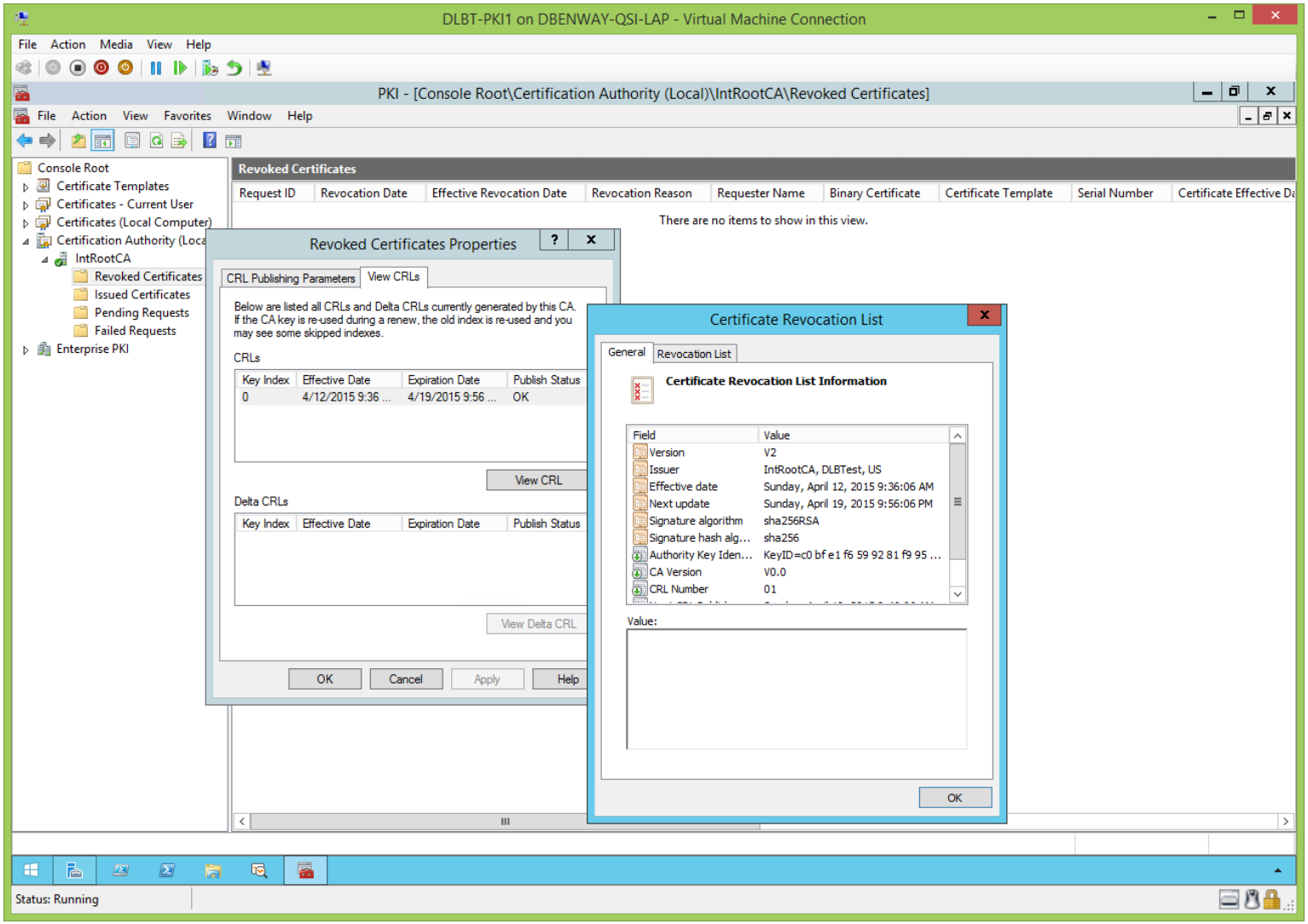
(jump to TOC)

These CRL parameters are properties of the root CA, and we'll change these later with CertUtil.exe.

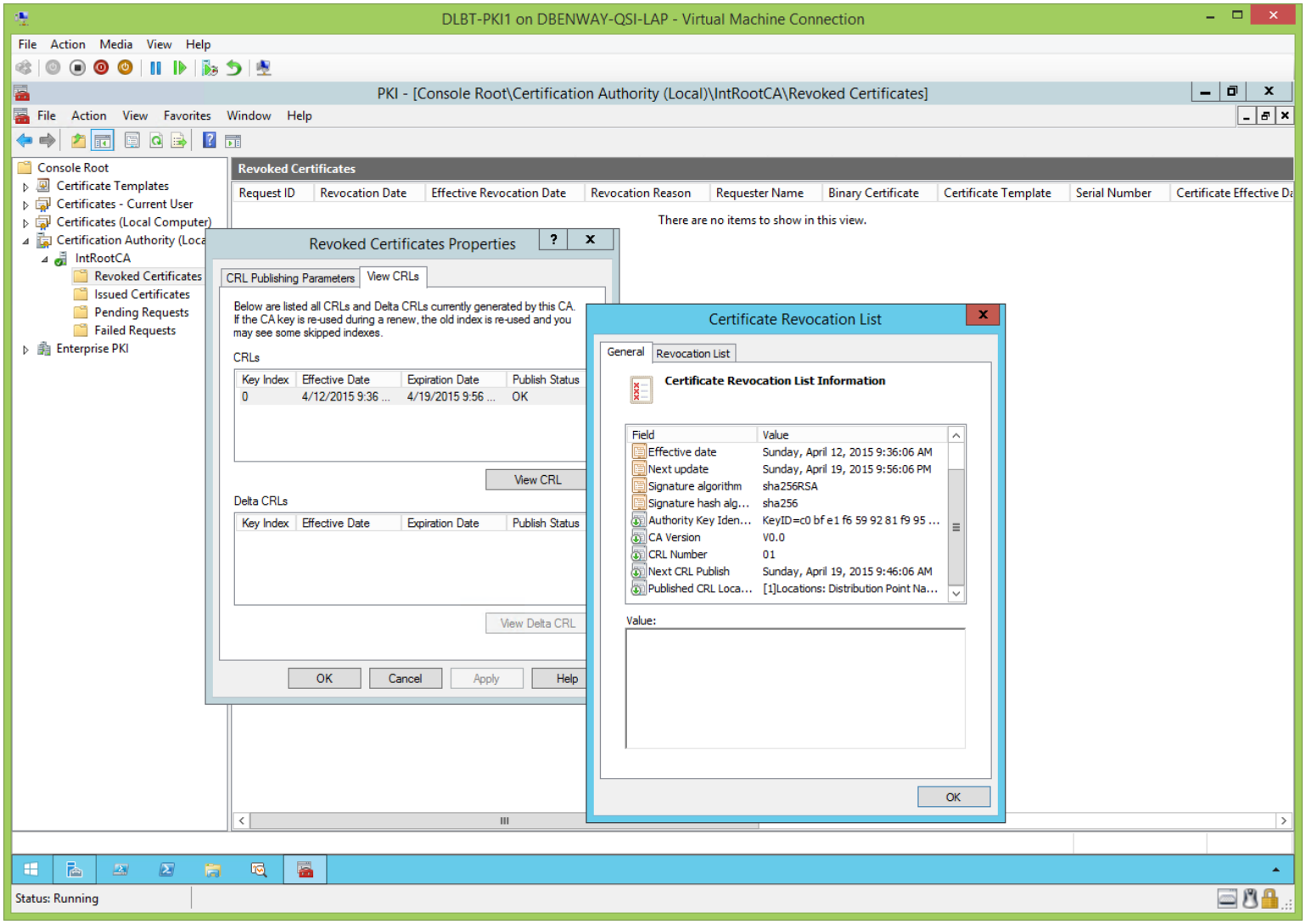


Note: by default, the standalone root CA does not publish delta CRLs (this was not set in the root CA's CAPolicy.inf, and we have not yet run the certUtil.exe commands).

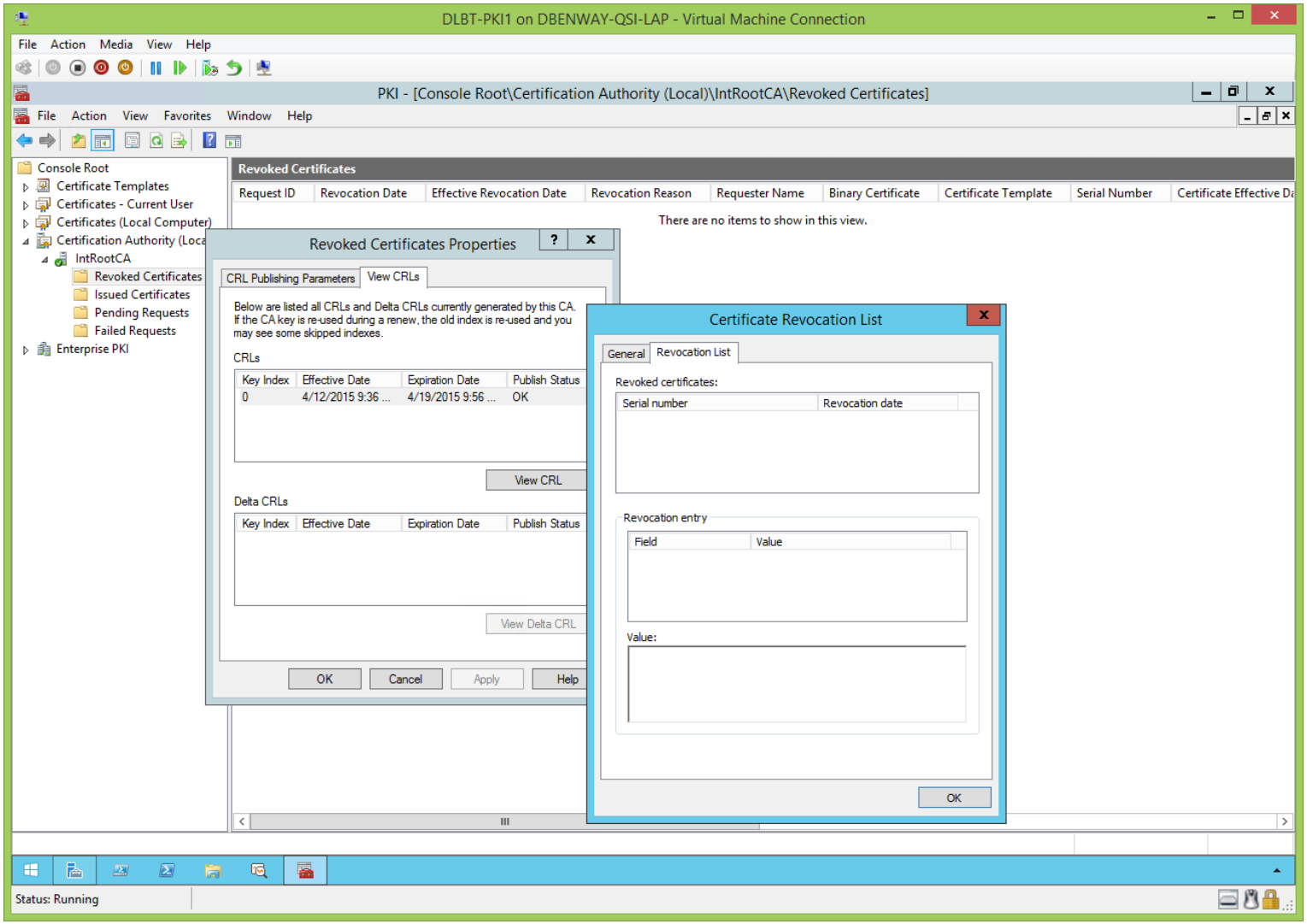
View the root CA's CRL properties, cont'd:



View the root CA's CRL properties, cont'd:



View the root CA's CRL properties, cont'd:



Root CA's Registry (Before CertUtil.exe):

(jump to TOC)

View the root CA's Registry:

DLBT-PKI1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

Registry Editor

File Edit View Favorites Help

bfadfcoei
bfadi
BFE
BITS
bowser
BrokerInfrastructure
Browser
bxfcoe
bxois
cdfs
cdrom
CertPropSvc
CertSvc
Configuration
IntRootCA
CSP
EncryptionCSP
ExitModules
PolicyModules
Performance
Security
cht4vbd
CLFS
clr_optimization_v4.0.30319_3
clr_optimization_v4.0.30319_6
CmBatt
CNG
CngHwAssist
CompositeBus
COMSysApp
condrv
crypt32
CryptSvc
DCLocator
DcomLaunch
defragsvc
DeviceAssociationService
DeviceInstall

Name	Type	Data
(Default)	REG_SZ	(value not set)
CACertHash	REG_MULTI_SZ	56 94 a3 26 2b 37 57 e9 e3 55 c1 f8 e3 45 ce 02 85 13 36 db
CACertPublicationURLs	REG_MULTI_SZ	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt 0:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11 0:http:/
CAServerName	REG_SZ	DLBT-PKI1
CAType	REG_DWORD	0x00000003 (3)
CAXchgCertHash	REG_MULTI_SZ	
CAXchgOverlapPeriod	REG_SZ	Days
CAXchgOverlapPeriodUnits	REG_DWORD	0x00000001 (1)
CAXchgValidityPeriod	REG_SZ	Weeks
CAXchgValidityPeriodUnits	REG_DWORD	0x00000001 (1)
CertEnrollCompatible	REG_DWORD	0x00000000 (0)
ClockSkewMinutes	REG_DWORD	0x0000000a (10)
CommonName	REG_SZ	IntRootCA
CRLDeltaOverlapPeriod	REG_SZ	Minutes
CRLDeltaOverlapUnits	REG_DWORD	0x00000000 (0)
CRLDeltaPeriod	REG_SZ	Days
CRLDeltaPeriodUnits	REG_DWORD	0x00000000 (0)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	c0 61 1c 2f a7 7a d0 01
CRLOverlapPeriod	REG_SZ	Hours
CRLOverlapUnits	REG_DWORD	0x00000000 (0)
CRLPeriod	REG_SZ	Weeks
CRLPeriodUnits	REG_DWORD	0x00000001 (1)
CRLPublicationURLs	REG_MULTI_SZ	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl 8:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6
EKUOIDsForPublishExpiredCertInCRL	REG_MULTI_SZ	1.3.6.1.5.5.7.3.3 1.3.6.1.4.1.311.61.1.1
Enabled	REG_DWORD	0x00000001 (1)
EnforceX500NameLengths	REG_DWORD	0x00000001 (1)
ForceTeletex	REG_DWORD	0x00000012 (18)
HighSerial	REG_DWORD	0x0000002a (42)
InterfaceFlags	REG_DWORD	0x00000641 (1601)
KRACertCount	REG_DWORD	0x00000000 (0)
KRACertHash	REG_MULTI_SZ	
KRAFlags	REG_DWORD	0x00000000 (0)
LogLevel	REG_DWORD	0x00000003 (3)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\IntRootCA

Status: Running

View the root CA's Registry, cont'd:

DLBT-PKI1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

Registry Editor

File Edit View Favorites Help

bfadfcoei
bfadi
BFE
BITS
bowser
BrokerInfrastructure
Browser
bxfcoe
bxois
cdfs
cdrom
CertPropSvc
CertSvc
Configuration
IntRootCA
CSP
EncryptionCSP
ExitModules
PolicyModules
Performance
Security
cht4vbd
CLFS
clr_optimization_v4.0.30319_3
clr_optimization_v4.0.30319_6
CmBatt
CNG
CngHwAssist
CompositeBus
COMSysApp
condrv
crypt32
CryptSvc
DCLocator
DcomLaunch
defragsvc
DeviceAssociationService
DeviceInstall

Name	Type	Data
CRLDeltaOverlapPeriod	REG_SZ	Minutes
CRLDeltaOverlapUnits	REG_DWORD	0x00000000 (0)
CRLDeltaPeriod	REG_SZ	Days
CRLDeltaPeriodUnits	REG_DWORD	0x00000000 (0)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	c0 61 1c 2f a7 7a d0 01
CRLOverlapPeriod	REG_SZ	Hours
CRLOverlapUnits	REG_DWORD	0x00000000 (0)
CRLPeriod	REG_SZ	Weeks
CRLPeriodUnits	REG_DWORD	0x00000001 (1)
CRLPublicationURLs	REG_MULTI_SZ	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl 8:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6
EKUOIDsForPublishExpiredCertInCRL	REG_MULTI_SZ	1.3.6.1.5.5.7.3.3 1.3.6.1.4.1.311.61.1.1
Enabled	REG_DWORD	0x00000001 (1)
EnforceX500NameLengths	REG_DWORD	0x00000001 (1)
ForceTeletex	REG_DWORD	0x00000012 (18)
HighSerial	REG_DWORD	0x0000002a (42)
InterfaceFlags	REG_DWORD	0x00000641 (1601)
KRACertCount	REG_DWORD	0x00000000 (0)
KRACertHash	REG_MULTI_SZ	
KRAFlags	REG_DWORD	0x00000000 (0)
LogLevel	REG_DWORD	0x00000003 (3)
MaxIncomingAllocSize	REG_DWORD	0x00010000 (65536)
MaxIncomingMessageSize	REG_DWORD	0x00010000 (65536)
PolicyFlags	REG_DWORD	0x00000000 (0)
Security	REG_BINARY	01 00 14 84 90 00 00 00 a0 00 00 00 14 00 00 00 44 00 00 00 02 00 30 00 02 00 00 00 02 c0 14 00 ff ff 00 00 01 01 00 00 00 00 00 01 00 00 00 00 02
SetupStatus	REG_DWORD	0x00000001 (1)
SignedAttributes	REG_MULTI_SZ	RequesterName
SubjectTemplate	REG_MULTI_SZ	EMail CommonName OrganizationalUnit Organization Locality State DomainComponent Country
UseDS	REG_DWORD	0x00000000 (0)
ValidityPeriod	REG_SZ	Years
ValidityPeriodUnits	REG_DWORD	0x00000001 (1)
ViewAgeMinutes	REG_DWORD	0x00000010 (16)
ViewIdleMinutes	REG_DWORD	0x00000008 (8)

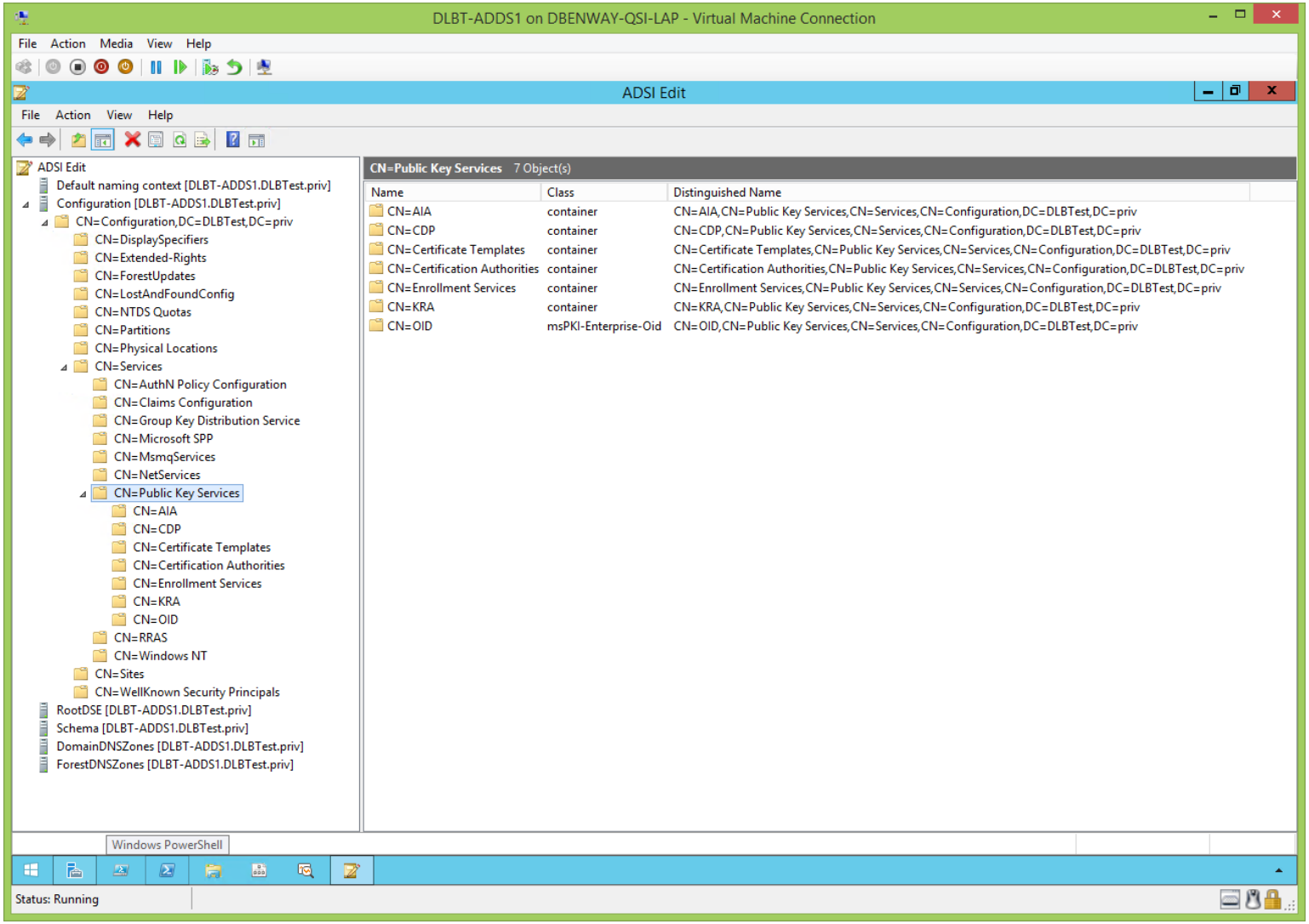
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\IntRootCA

Status: Running

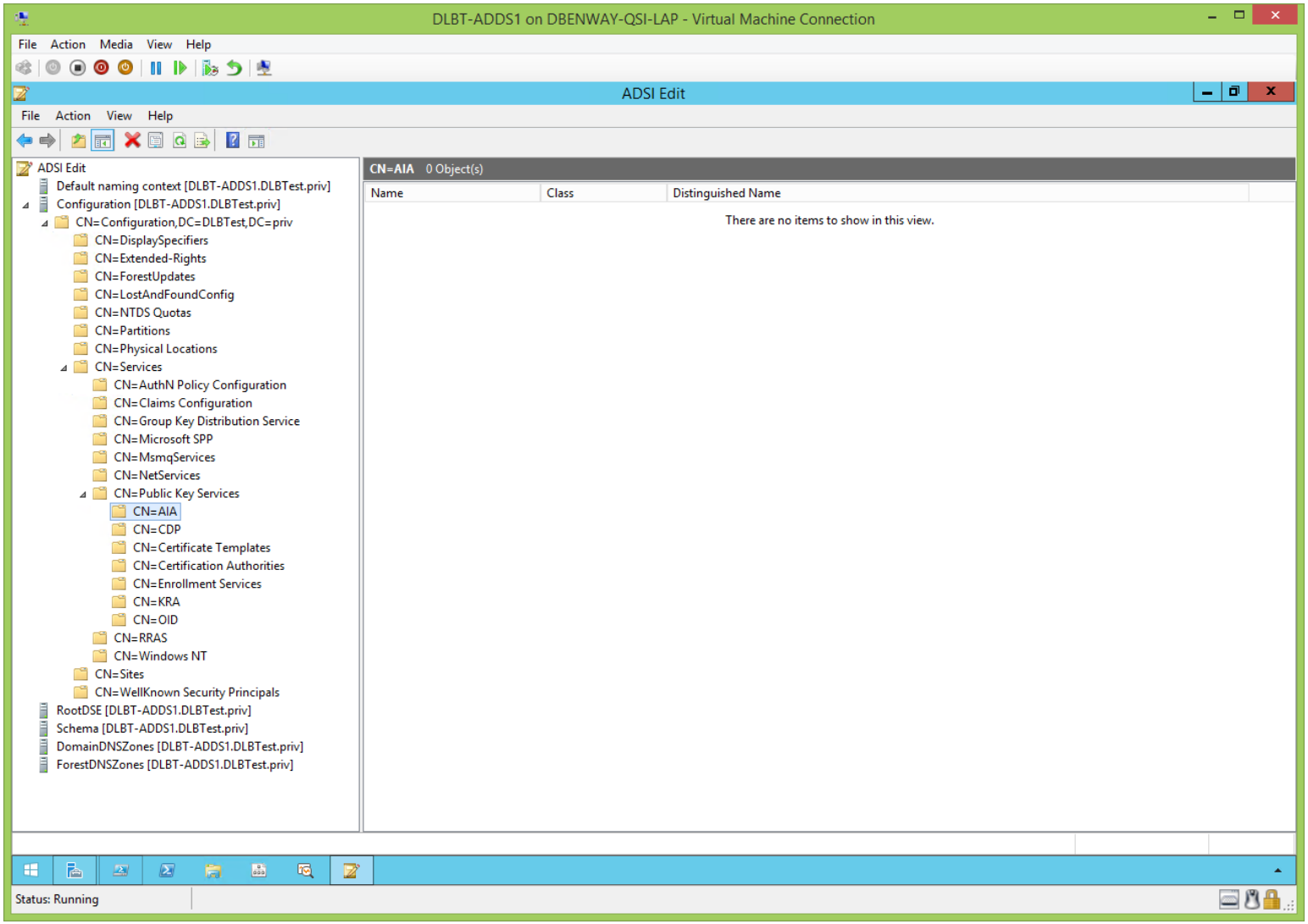
ADSIEdit.msc (Before CertUtil.exe):

(jump to TOC)

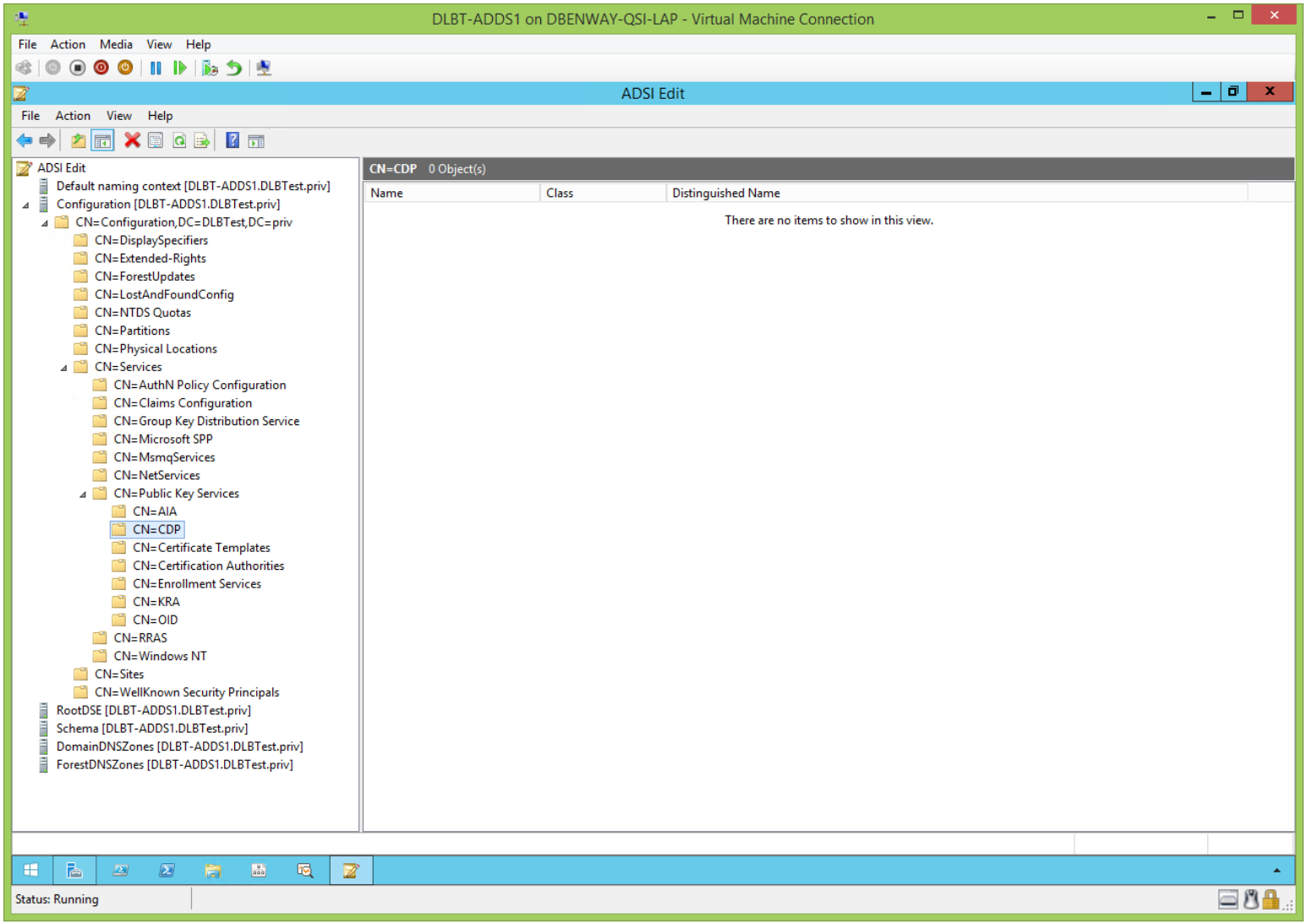
All 'Public Key Services' folders in ADSIEdit.msc are empty because the root is neither on the network nor a Domain member:



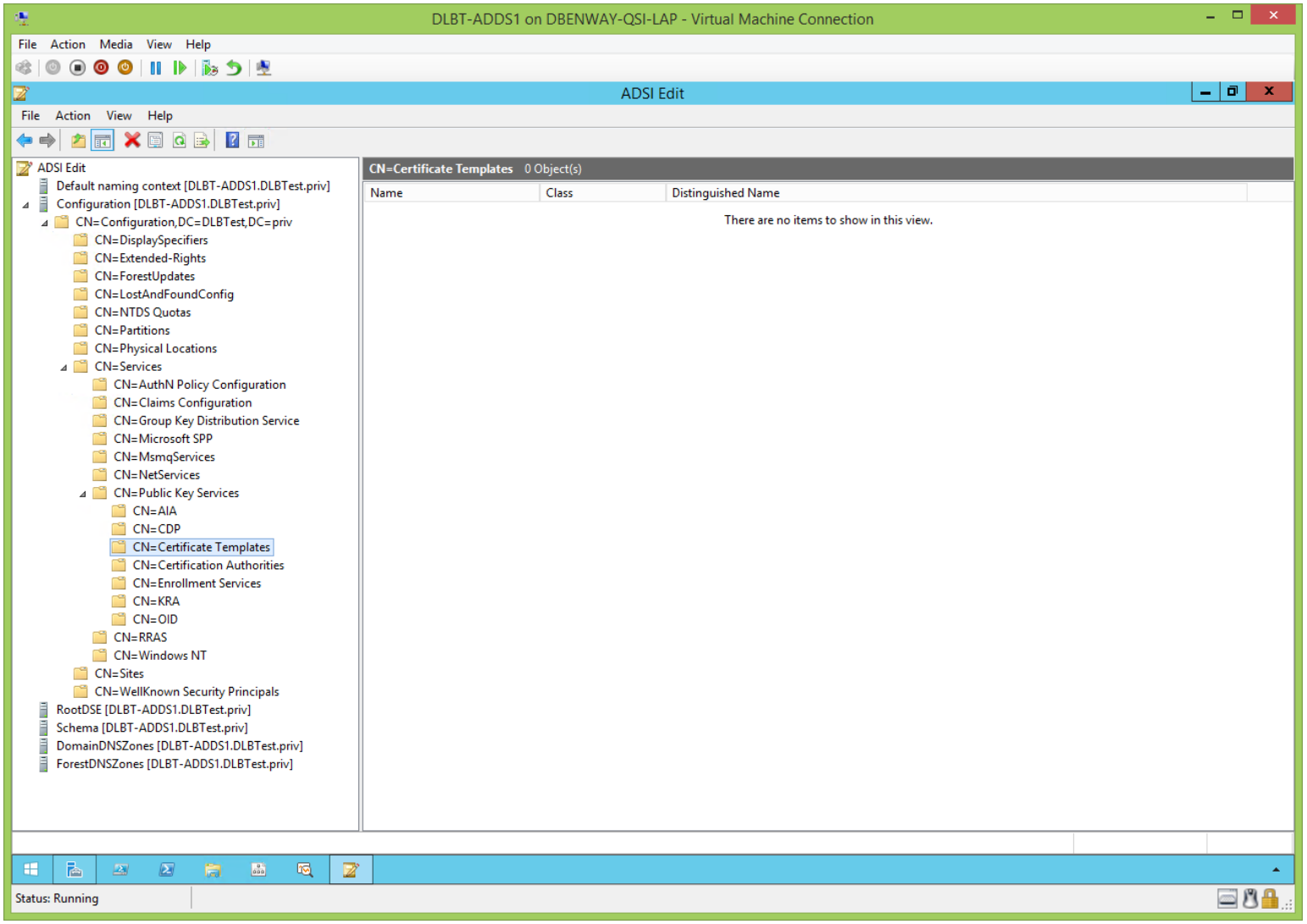
View ADSIEdit.msc, cont'd:



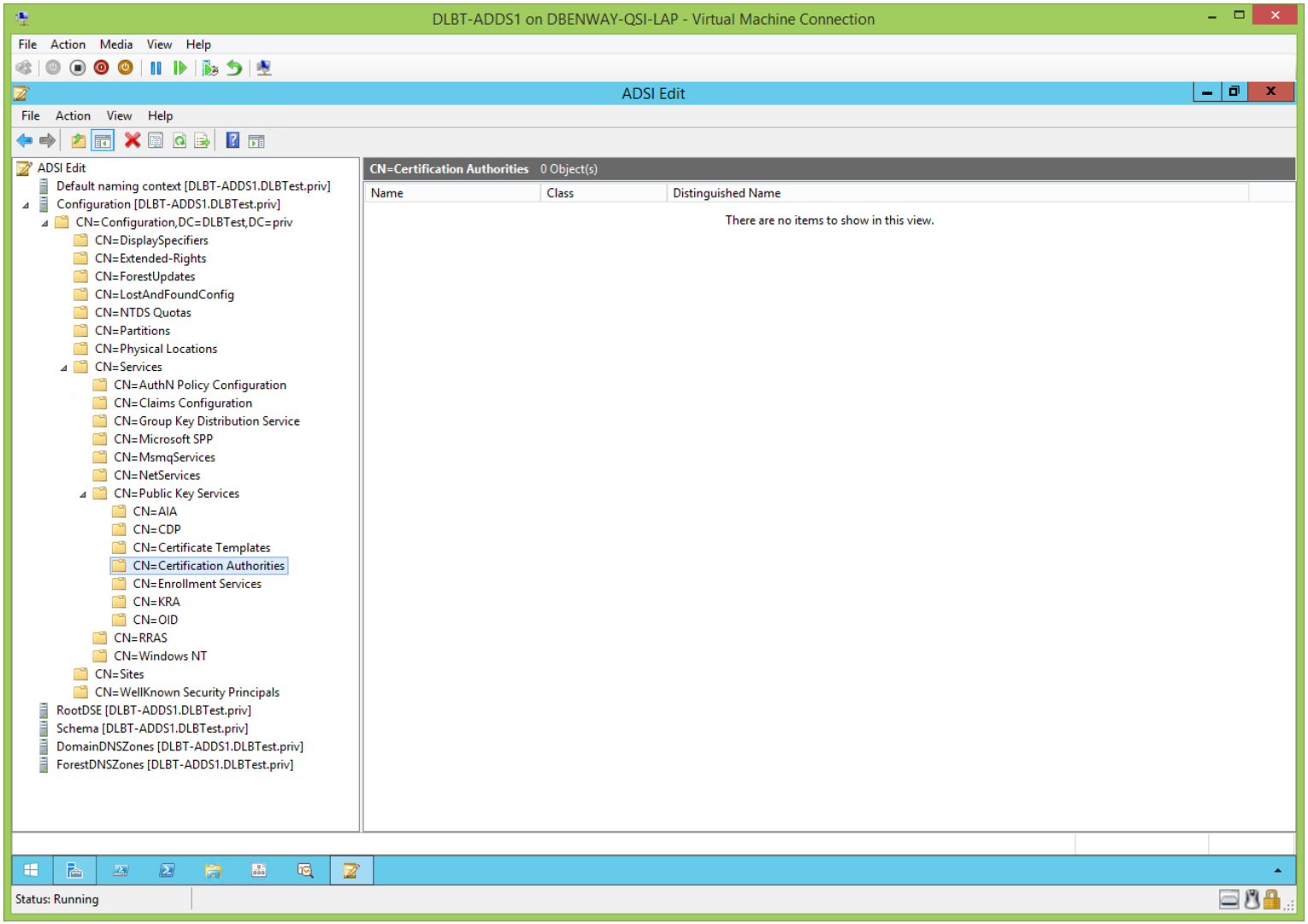
View ADSIEdit.msc, cont'd:



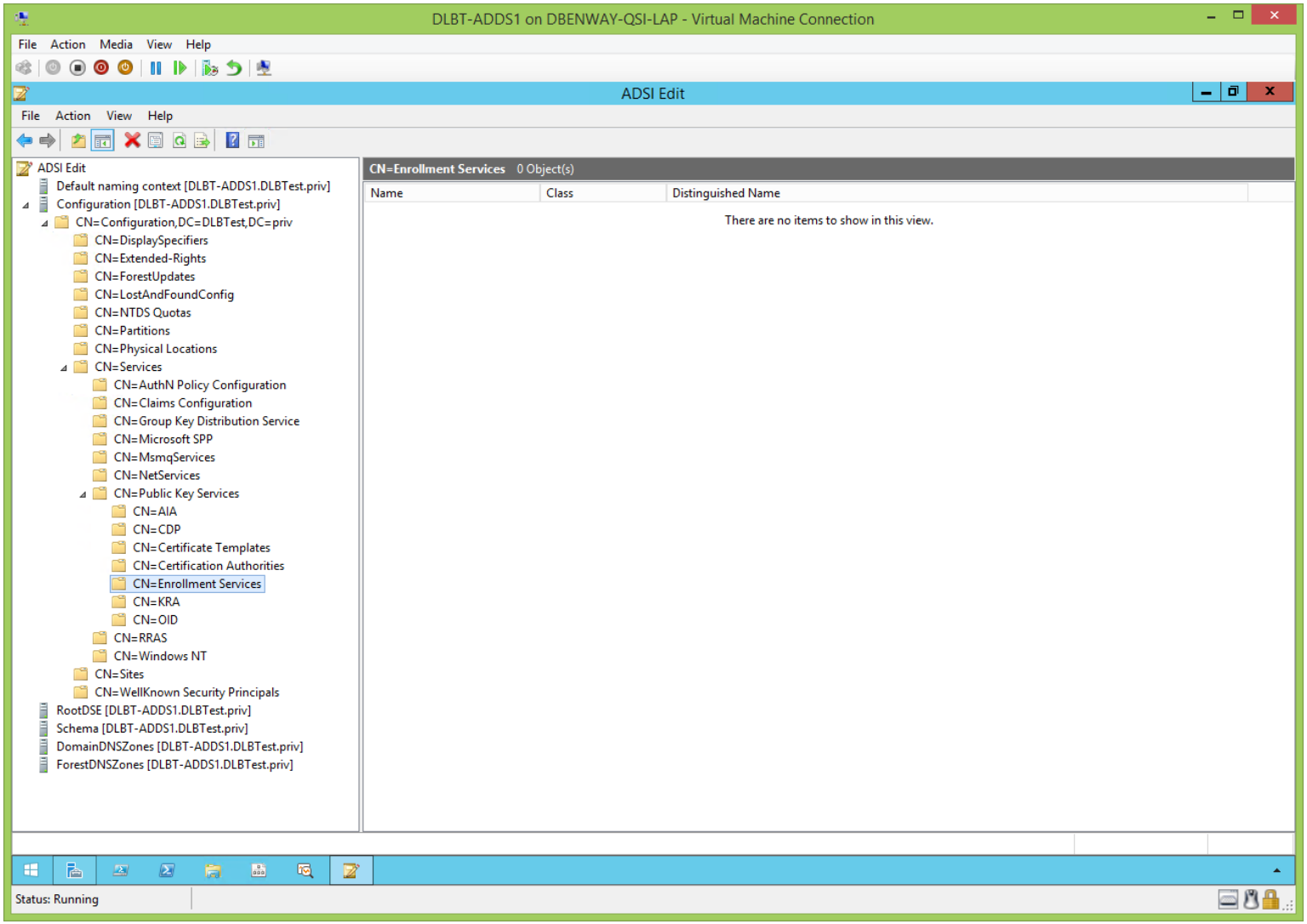
View ADSIEdit.msc, cont'd:



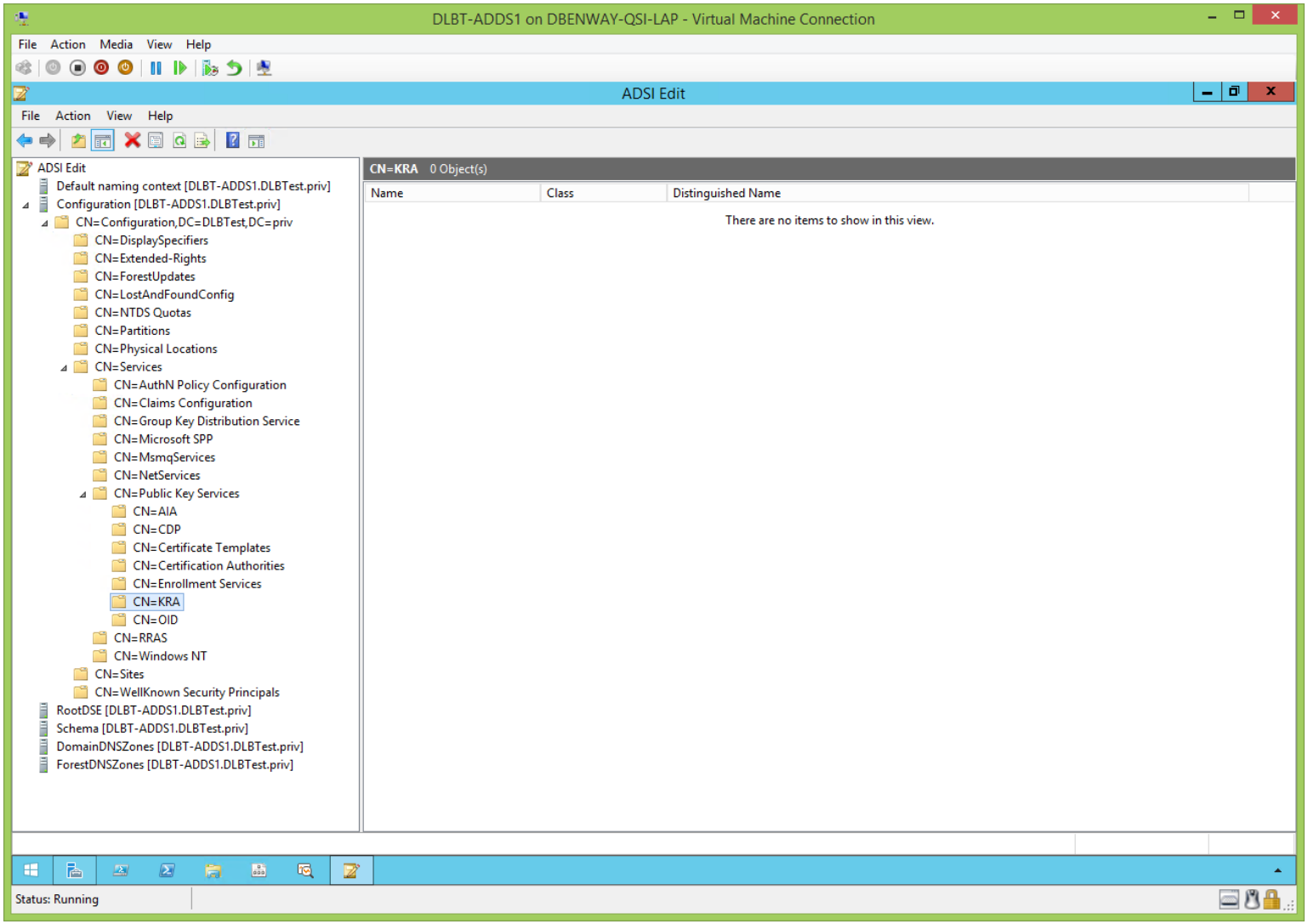
View ADSIEdit.msc, cont'd:



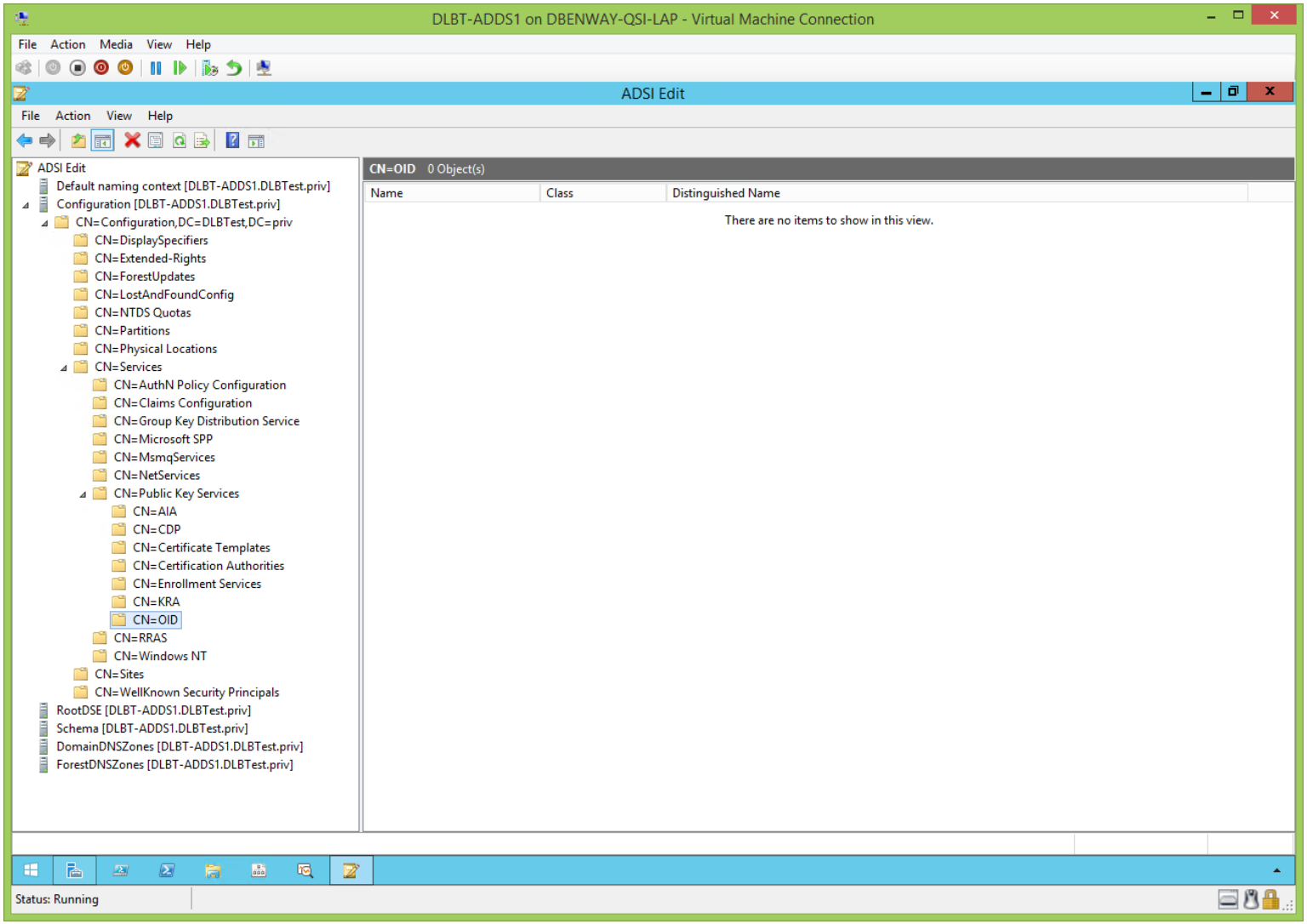
View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:



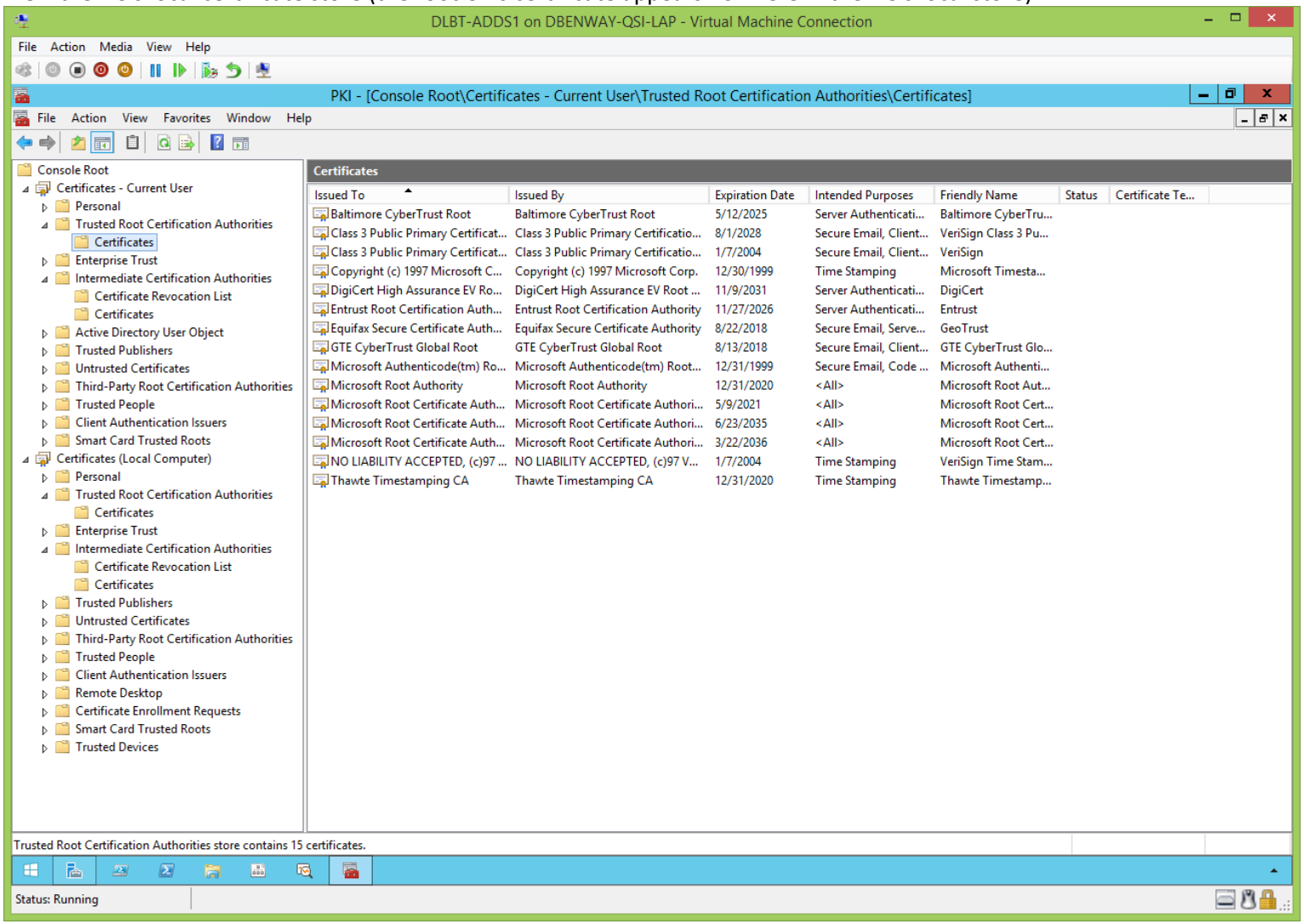
View ADSIEdit.msc, cont'd:



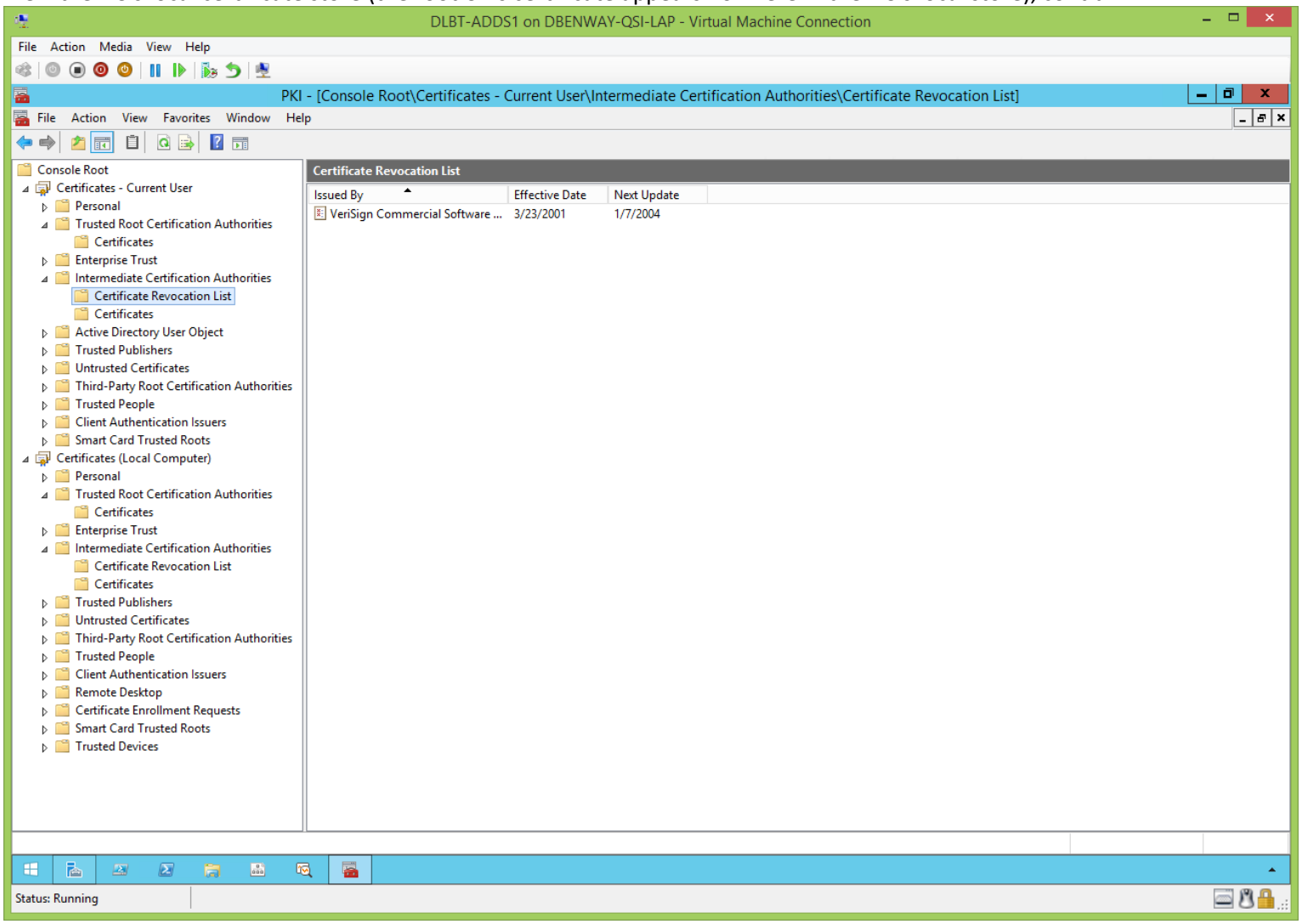
DC's Local Certificate Store (Before CertUtil.exe):

(jump to TOC)

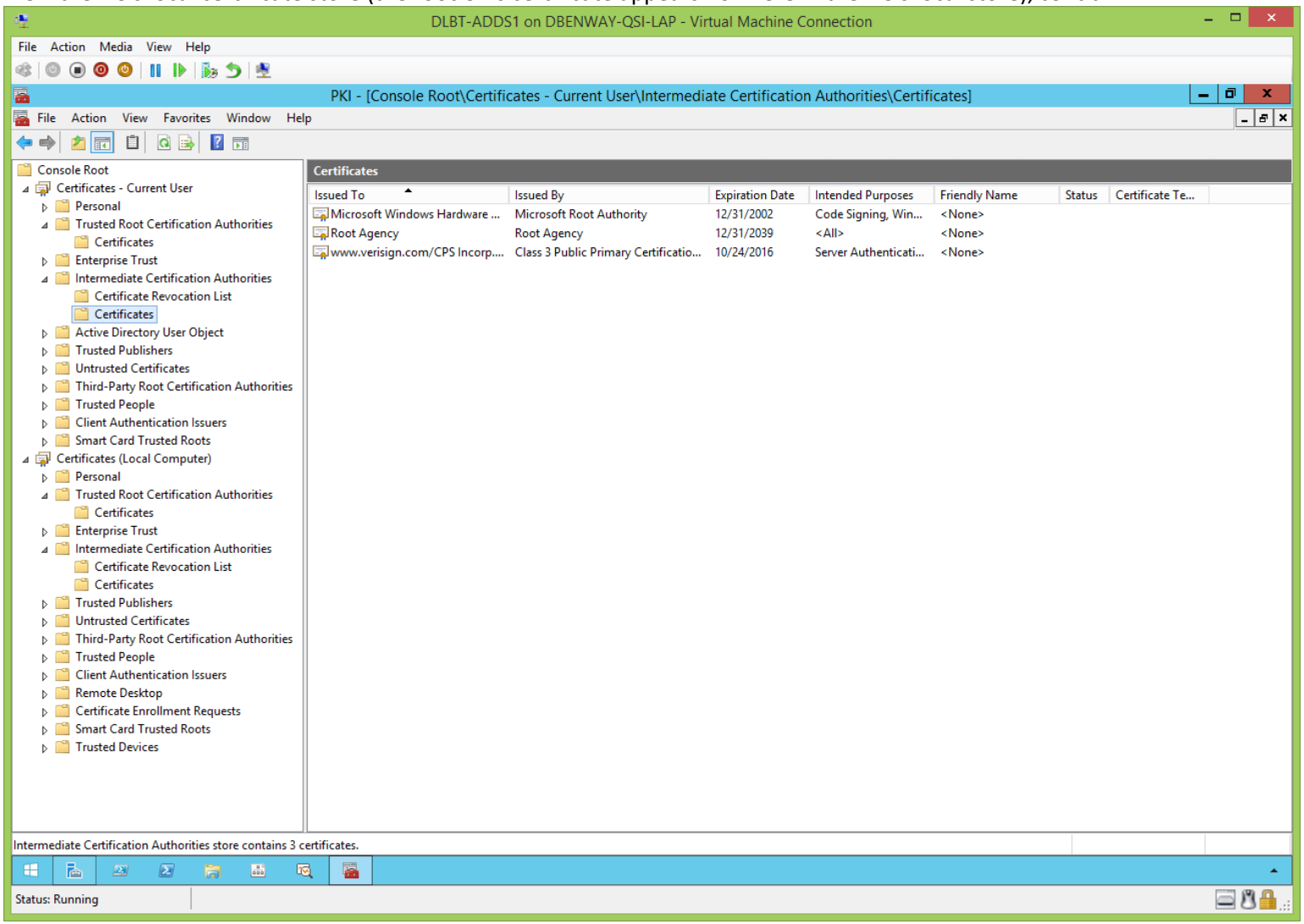
View the DC's local certificate store (the root CA's certificate appears nowhere in the DC's local store):



View the DC's local certificate store (the root CA's certificate appears nowhere in the DC's local store), cont'd:



View the DC's local certificate store (the root CA's certificate appears nowhere in the DC's local store), cont'd:



View the DC's local certificate store (the root CA's certificate appears nowhere in the DC's local store), cont'd:

DLBT-ADDS1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

PKI - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Smart Card Trusted Roots
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices

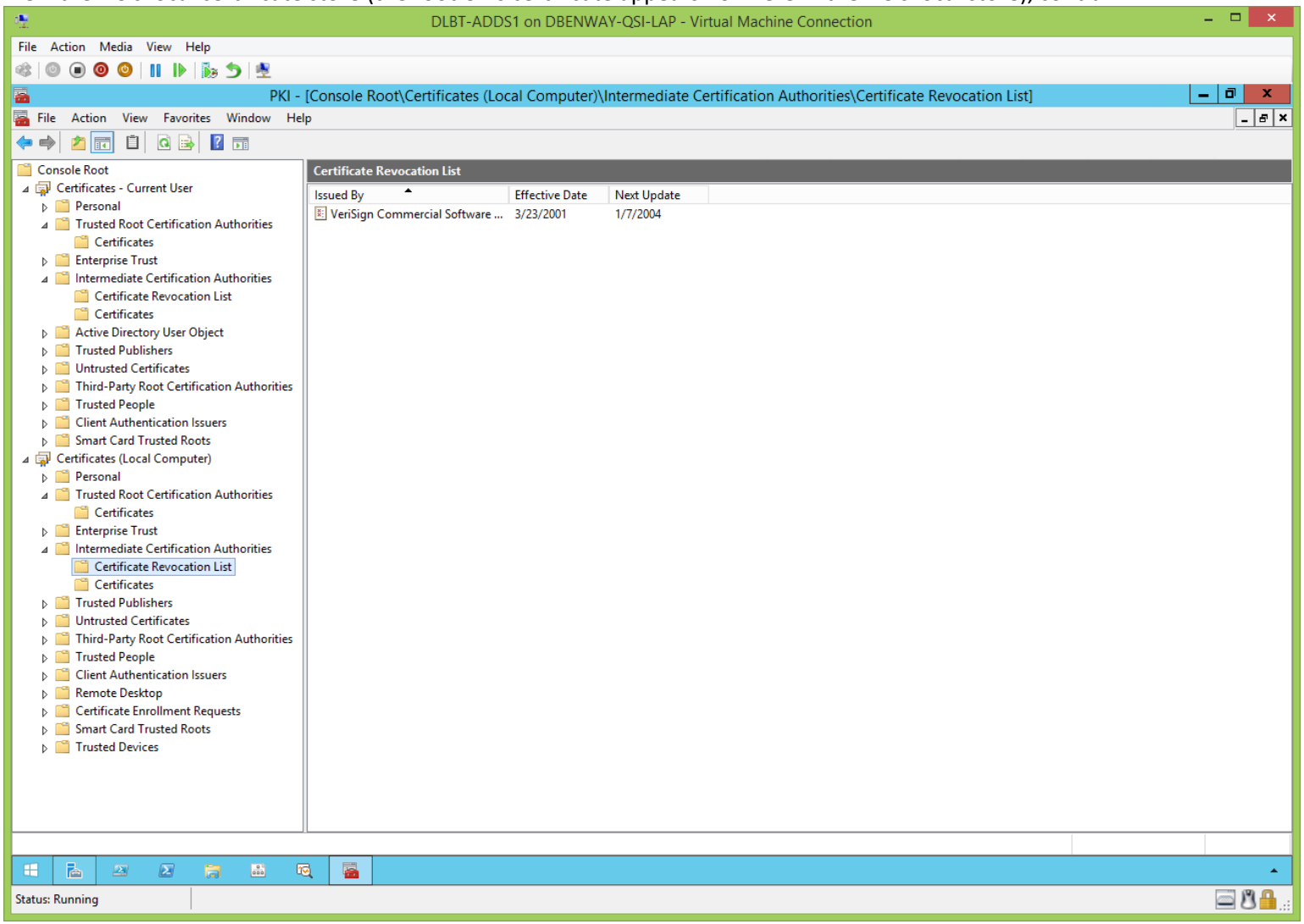
Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	Baltimore CyberTru...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
Entrust Root Certification Auth...	Entrust Root Certification Authority	11/27/2026	Server Authenticati...	Entrust		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		

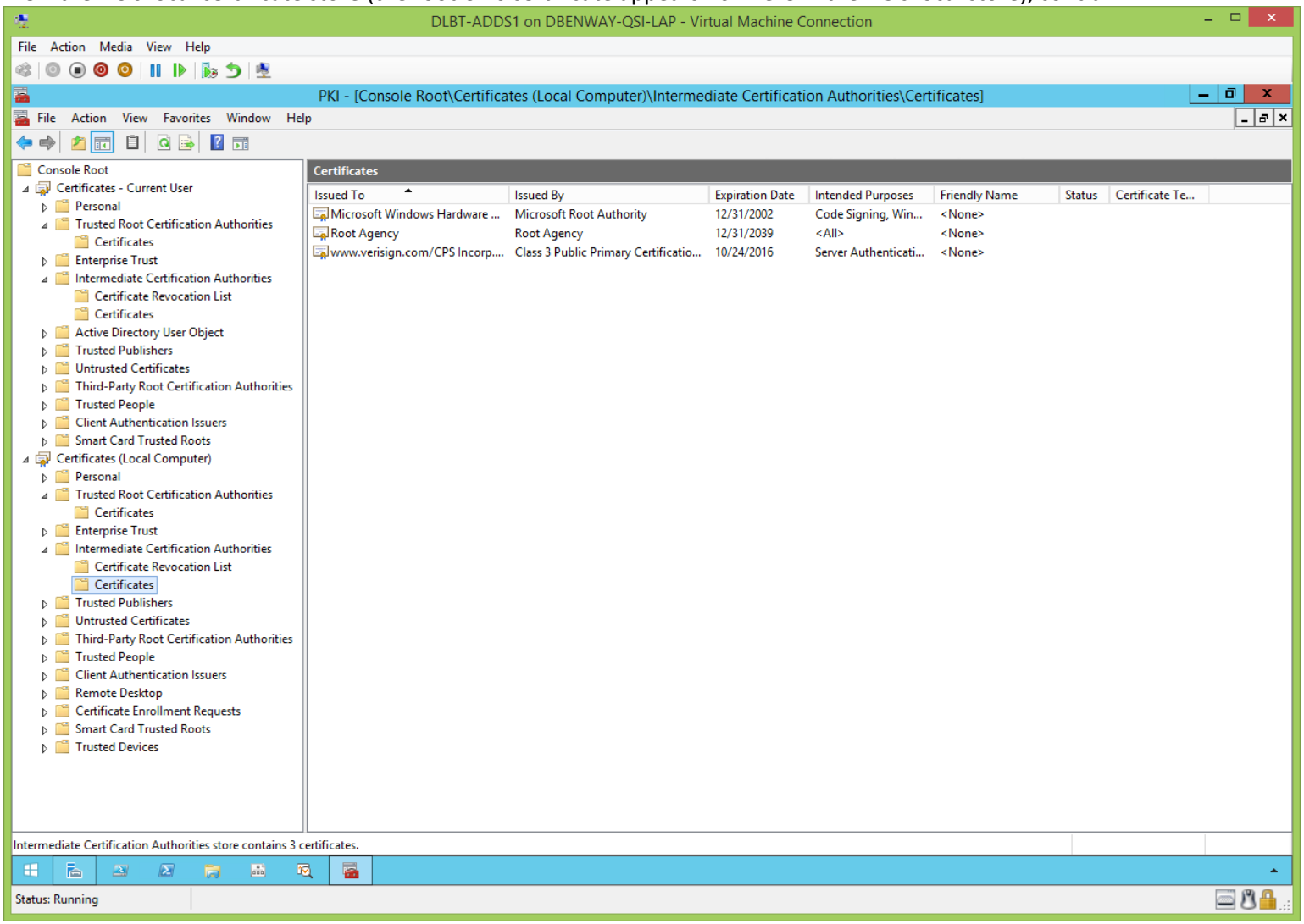
Trusted Root Certification Authorities store contains 15 certificates.

Status: Running

View the DC's local certificate store (the root CA's certificate appears nowhere in the DC's local store), cont'd:



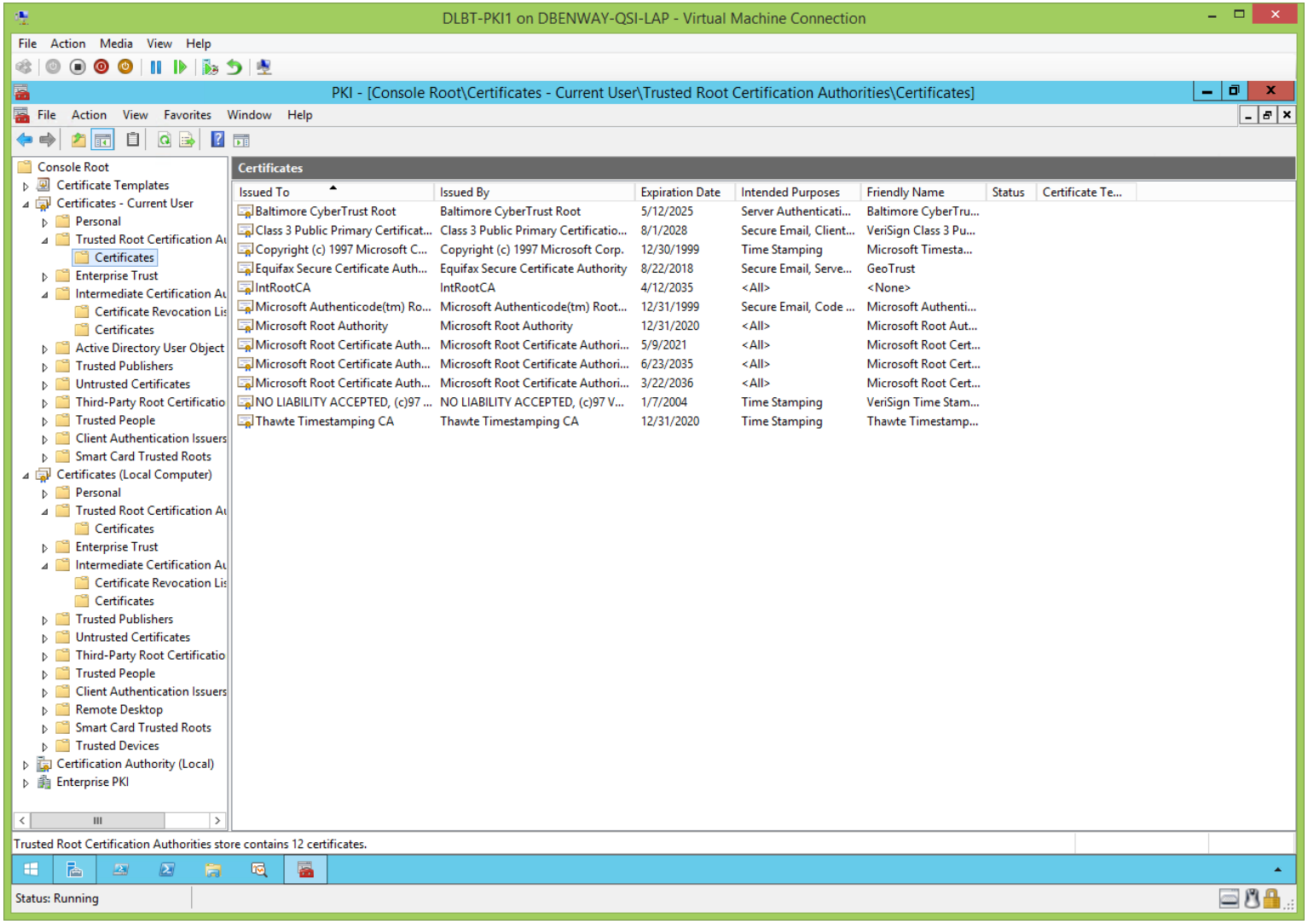
View the DC's local certificate store (the root CA's certificate appears nowhere in the DC's local store), cont'd:



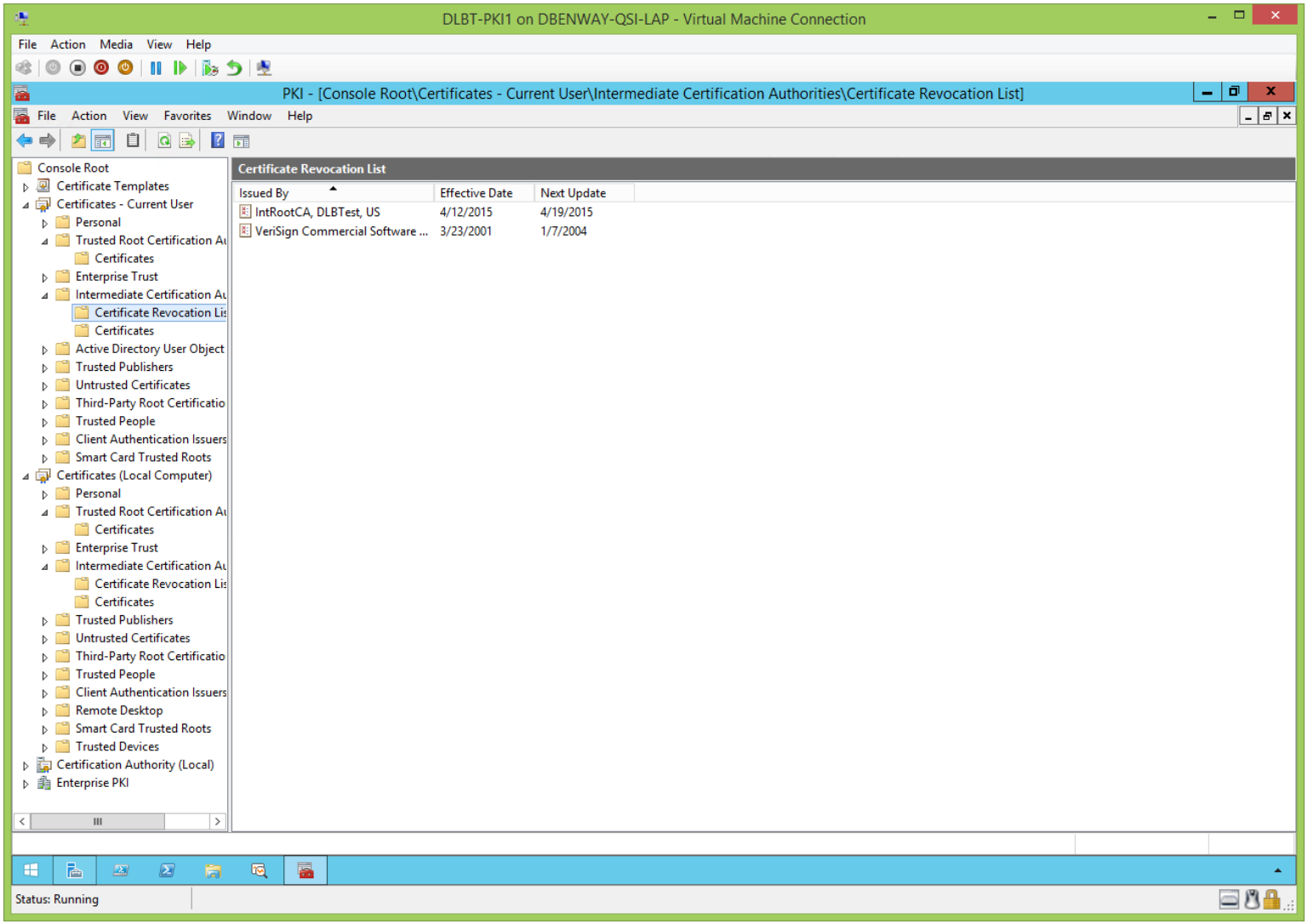
Root CA's Local Certificate Store (Before CertUtil.exe):

(jump to TOC)

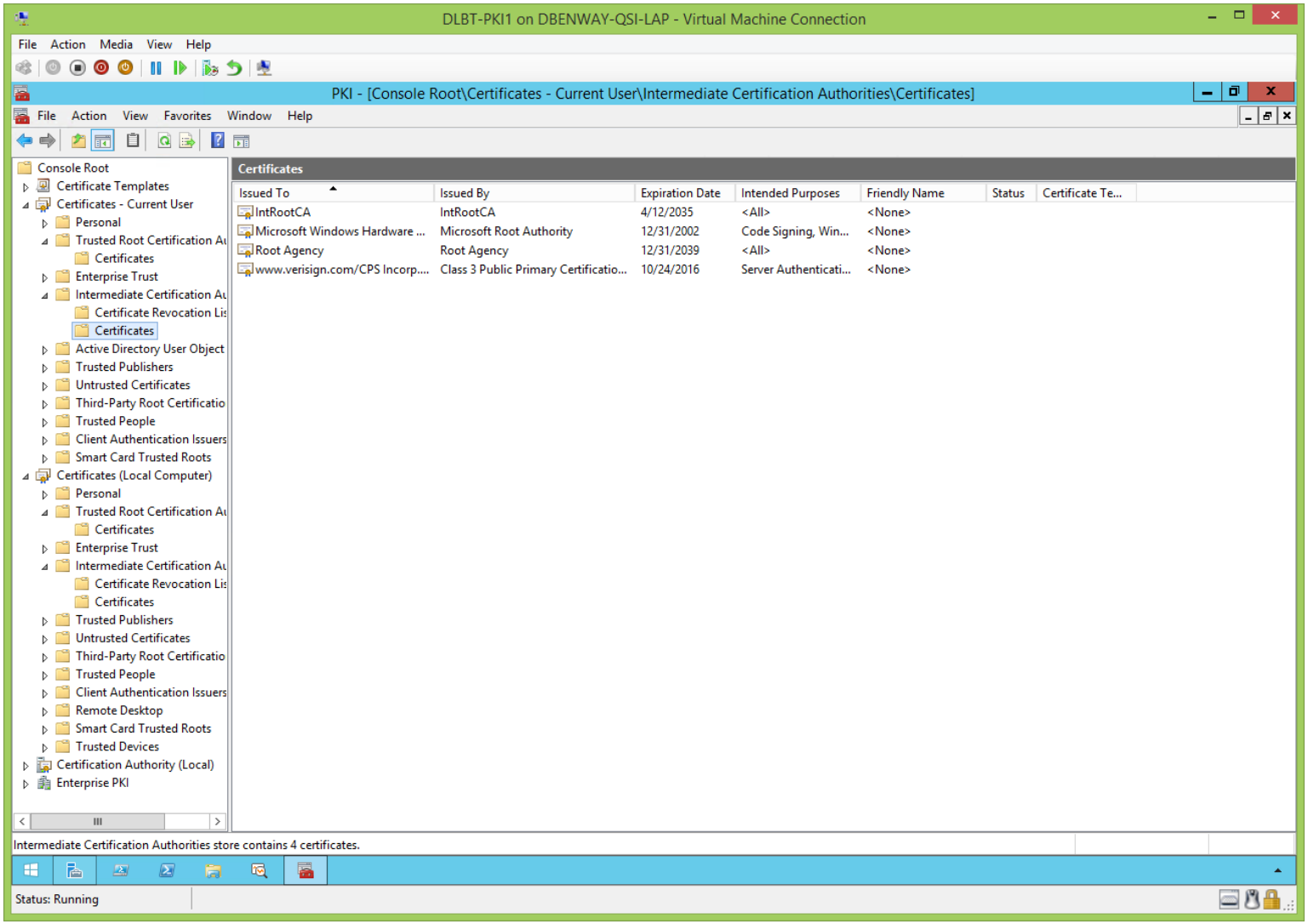
View the root CA's local certificate store:



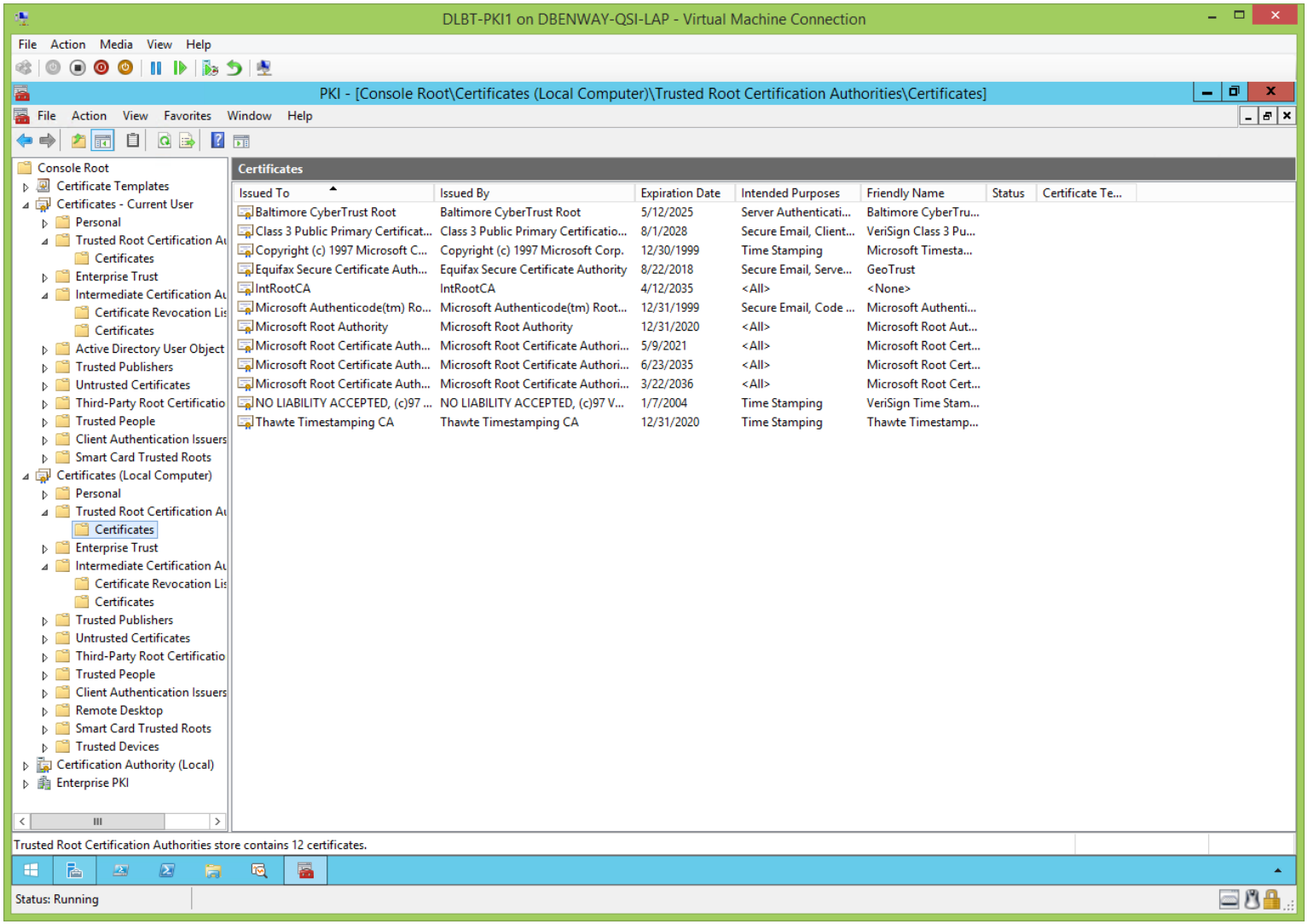
View the root CA's local certificate store, cont'd:



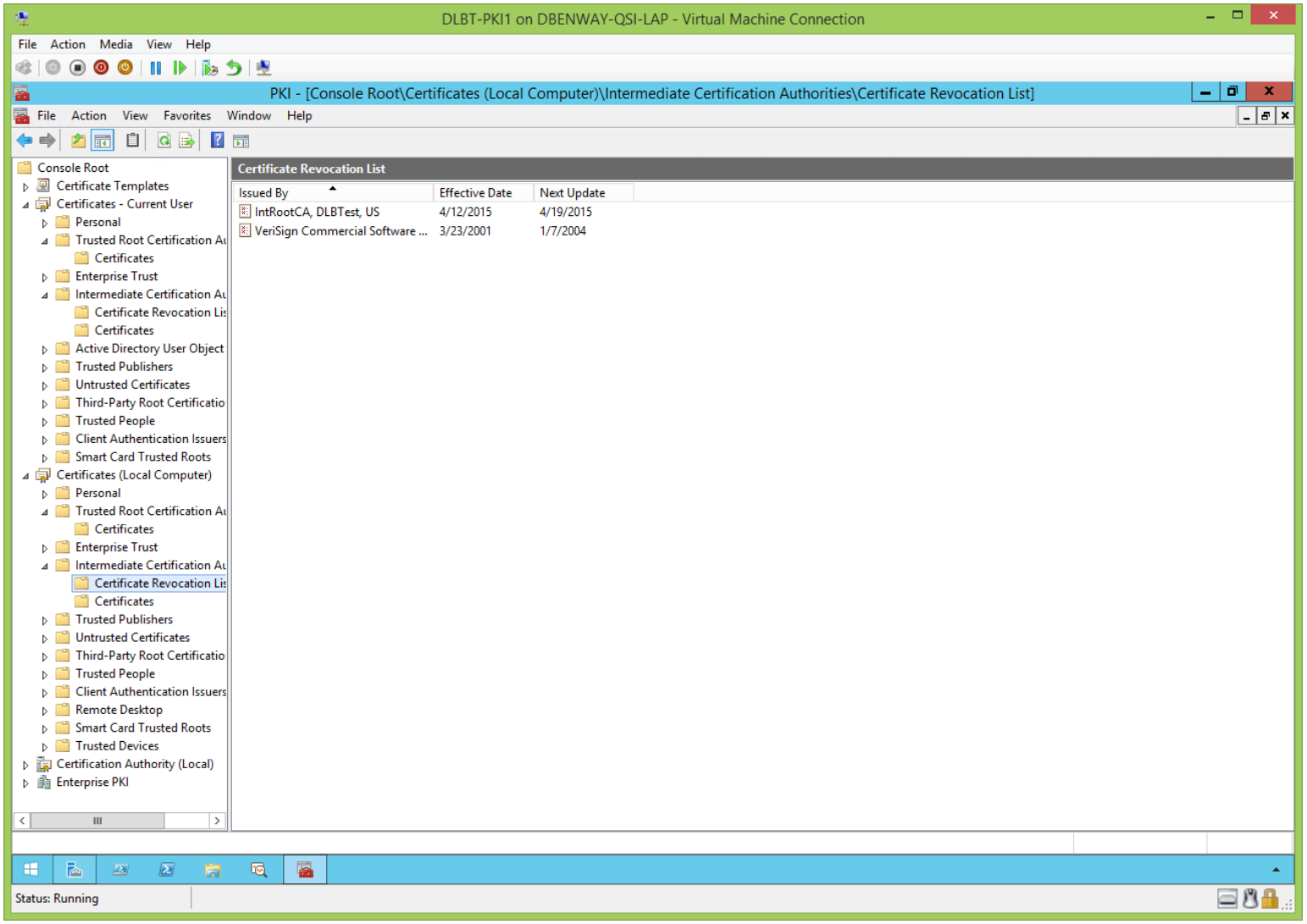
View the root CA's local certificate store, cont'd:



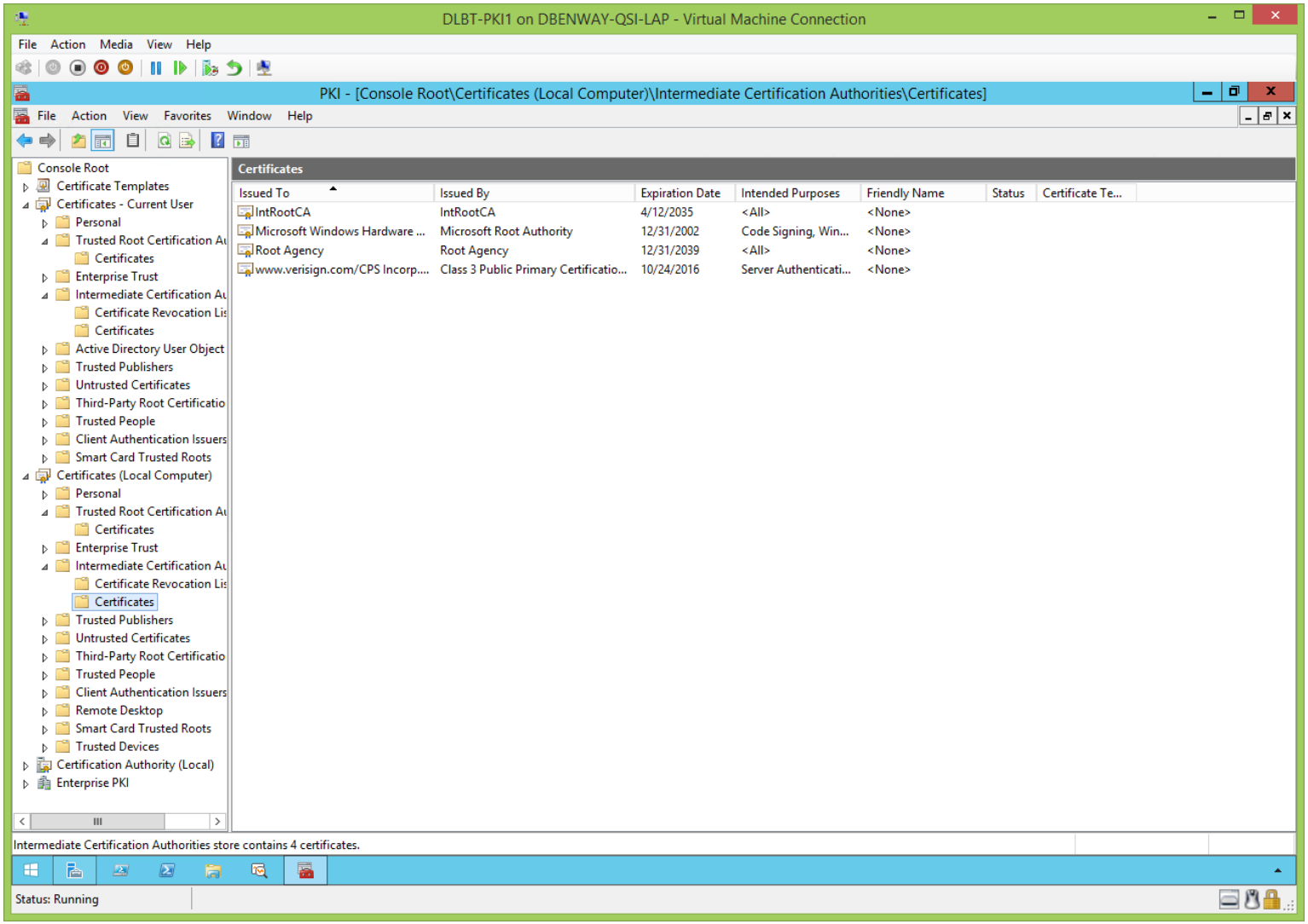
View the root CA's local certificate store, cont'd:



View the root CA's local certificate store, cont'd:



View the root CA's local certificate store, cont'd:



Root CA's CertUtil.exe:

(jump to TOC)

WARNING: This file of CertUtil.exe commands has a lot of important comments that need to be read and understood, or problems will arise.
Note: Because the CAPolicy.inf and Certutil.exe files in this document have been updated since initial publication, the values in this document's screenshots (such as registry settings, publication intervals, etc.) might not always reflect the values from these files.

Now we'll run CertUtil.exe commands from an Administrator command prompt on the root CA to configure the root CA (be sure to read and follow the steps in the REM comments):

```
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | CertUtil Root
REM |
REM | Run these commands interactively from an administrative command prompt.
REM | Note: Although this file is written in batch form it is not intended to be run as a batch file, but to have its chunks of code individually copied
REM | and pasted into a command line.
REM | Note: If you run this as a batch you'll need to replace % with %%, and maybe create a 'wait' when restarting services.
REM | Note: If you run this as a batch you'll still need to manually copy this root CA's certificate to a thumb drive and publish it to AD.
REM | Note: If you run this as a batch you'll still need to manually copy this root CA's certificate, and the base and the delta CRL this root CA generates
REM | to a thumb drive and publish them to the CDP.
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Enable all auditing events for this root CA.
REM | Note: This can also be done from the 'Auditing' tab of this root CA's properties sheet in PKI.mmc, but better to turn it on early right after ADCS
REM | installation.
REM | Also be sure to use SecPol.msc to track Success and Failure in 'Advanced Audit Policy Configuration' > 'System Audit Policies' >
REM | 'Object Access' > Audit Certification Services.
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\AuditFilter 127

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Specify the Forest's configuration partition.
REM | This is only needed if the root is online, and if citing LDAP URLs for AIA and/or CDP (which is no longer best practice!) but include it just in case.
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\DSConfigDN CN=Configuration,DC=DLBTest,DC=priv

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Set the validity period for the certificates this root CA issues (not for this root CA's certificate).
REM | Note: Standalone CAs configure validity periods for the certificates they issue in their registry, enterprise CAs do it in their templates (and
REM | if not there then it defaults to their registry).
REM | Note: The lowest certificates should have up to 5 years, so the sub/policy/issuing CA is 10, so this root CA is 20.
REM | Note: the validity period for this root CA's certificate is set during its ADCS installation wizard, and also in its CAPolicy.inf file's 'renewal'
REM | parameters
REM | Note: the validity period of the sub/policy/issuing CA's certificate is set during its ADCS installation wizard, and also in its CAPolicy.inf file's
REM | 'renewal' parameters
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\ValidityPeriodUnits 10
certUtil.exe -setReg CA\ValidityPeriod "years"

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Define the publication intervals for the base and the delta CRL this root CA generates.
REM | Note: CRLOverlap parameters in CAPolicy.inf are ignored.
REM | Note: CRLOverlap cannot be greater than CRLPeriod.
```

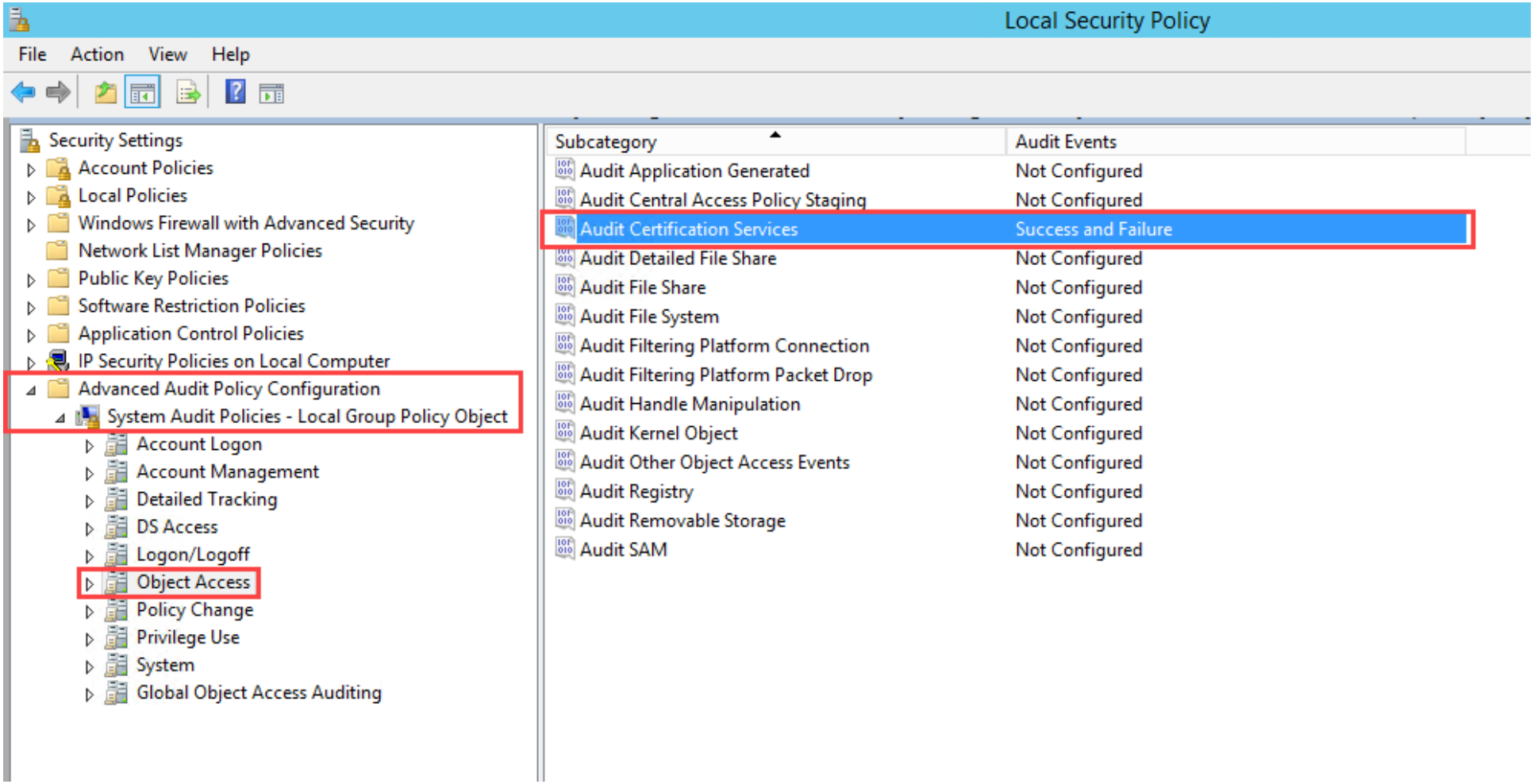
```
REM | Note: This is a lab environment which is offline for extended periods, so these values are unusually large, and a delta CRL is not used.
REM | http://blogs.technet.com/b/xdot509/archive/2012/11/26/pki-design-considerations-certificate-revocation-and-crl-publishing-strategies.aspx
REM |        PKI Design Considerations: Certificate Revocation and CRL Publishing Strategies
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\CRLPeriodUnits 24
certUtil.exe -setReg CA\CRLPeriod "months"
certUtil.exe -setReg CA\CRLOverlapUnits 1
certUtil.exe -setReg CA\CRLOverlapPeriod "months"
REM |-----------------------------------------------
certUtil.exe -setReg CA\CRLDeltaPeriodUnits 0
certUtil.exe -setReg CA\CRLDeltaPeriod "days"
certUtil.exe -setReg CA\CRLDeltaOverlapUnits 0
certUtil.exe -setReg CA\CRLDeltaOverlapPeriod "days"

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Set the CDP extension URLs for the certificates this root CA issues (not for this root CA's certificate).
REM | This root CA is issuing a certificate for only the sub/policy/issuing CA.
REM | This root CA is offline, so no need to publish to anything but the local file system.
REM | You can use certUtil.exe or the GUI to set these URLs. Komar p. 115 describes the numeric codes used, but they should be (top to bottom):
REM | '1,8,4,2,64,128'.
REM | 65 means 1st and 5th checkboxes in this root CA's CRL extensions GUI, 134 means 3rd, 4th, and 6th checkboxes in this root CA's CRL extensions GUI.
REM | \n means new line (see Appendix A).
REM | %3 = CAName, %8 = CRLNameSuffix, %9 = DeltaCRLAllowed
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\CRLPublicationURLs "65:%windir%\system32\CertSrv\CertEnroll\%3%8%9.crl\n134:http://PKI.DLBTest.priv/CDP/%3%8%9.crl"

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Set the AIA extension URLs for the certificates this root CA issues (not for this root CA's certificate).
REM | This root CA is issuing a certificate for only the sub/policy/issuing CA.
REM | This root CA is offline, so no need to publish to anything but the local file system.
REM | You can use certUtil.exe or the GUI to set these URLs. Komar p. 116 describes the numeric codes used, but '1' doesn't seem valid?
REM | 0 means no checkboxes in this root CA's AIA extensions GUI, 2 means the 1st checkbox in this root CA's AIA extensions GUI.
REM | \n means new line (see Appendix A).
REM | %1 = ServerDNSName, %3 = CAName, %4 = CertificateName
REM | Note: most sources recommend not using the '%1_' in the AIA extension URLs to create security through obscurity (see Appendix B).
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\CACertPublicationURLs "0:%windir%\system32\CertSrv\CertEnroll\%3%4.crt\n2:http://PKI.DLBTest.priv/AIA/%3%4.crt"

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM |Restart Certificate Services so the above changes take effect
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
net stop CertSvc & net start CertSvc

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Publish this root CA's base CRL and delta CRL (to whatever this CA's CDP extensions specify).
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -CRL

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Publish this root CA's certificate to AD for automatic distribution to Domain members (this is not the same as auto-enrollment):
REM |            Copy this root CA's certificate (%windir%\system32\certsrv\certenroll\*.crt) to a thumb drive.
REM |            From a Domain member system (with or without ADCS installed) run this command interactively from an administrative command prompt as an
REM |            Enterprise Admin:certUtil.exe -dspublish -f RootCACertFileName.crt RootCA
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Publish to the CDP this root CA's certificate:
REM |            Copy this root CA's %windir%\system32\CertSrv\CertEnroll\*.crt to the CDP's C:\IntePub\PKI\AIA
REM | Publish to the CDP this root CA's base CRL and delta CRL:
REM |            Copy this root CA's %windir%\system32\CertSrv\CertEnroll\*.crl to the CDP's C:\IntePub\PKI\CDP
```

```
REM |
REM | Note: publish to the CDP this root CA's base and delta CRL again after this root CA issues a certificate to the sub/policy/issuing CA.
REM |------------------------------------------------------------------------------------------------------------------------------------
```

Finish Enabling Auditing on the Root CA (After CertUtil.exe):

(jump to TOC)

In addition to the '`certUtil.exe -setReg CA\AuditFilter 127`' command, finish enabling auditing on the root CA using SecPol.msc as follows:



Root CA Manually Publish Certificate to AD (After CertUtil.exe):

(jump to TOC)

Be sure to follow the steps at the bottom of the root CA's CertUtil commands file.

The root CA's certificate should be published to AD as soon as practical so that it can get distributed quickly.

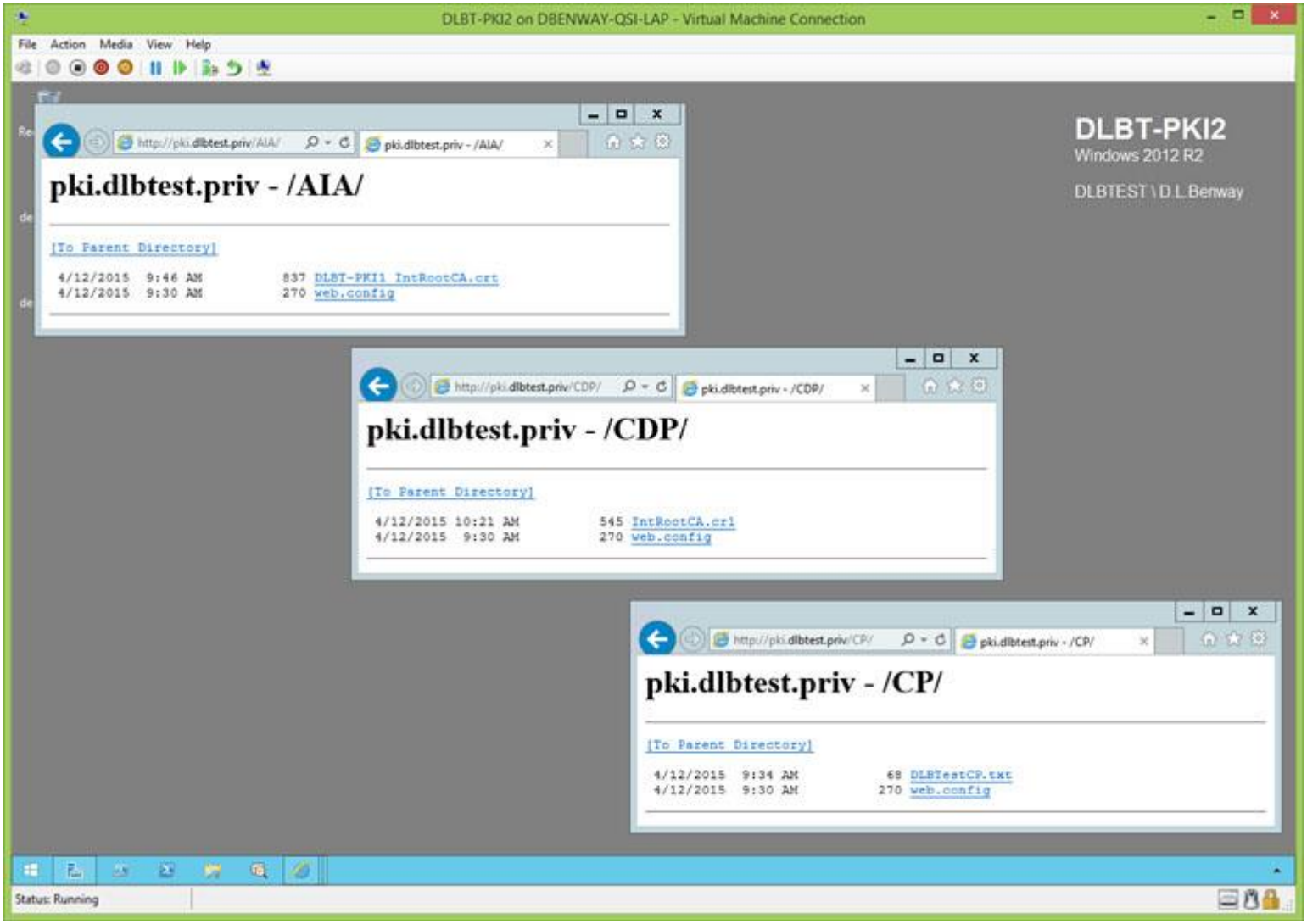
Root CA Manually Publish CRL and Certificate to the CDP (After CertUtil.exe):

(jump to TOC)

Be sure to follow the steps at the bottom of the root CA's CertUtil commands file.

Verify AIA, CDP, and CPS URLs' Content (After CertUtil.exe):

(jump to TOC)



Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's certificate filename contains the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

Root CA's Enterprise PKI Snap-In (After CertUtil.exe):

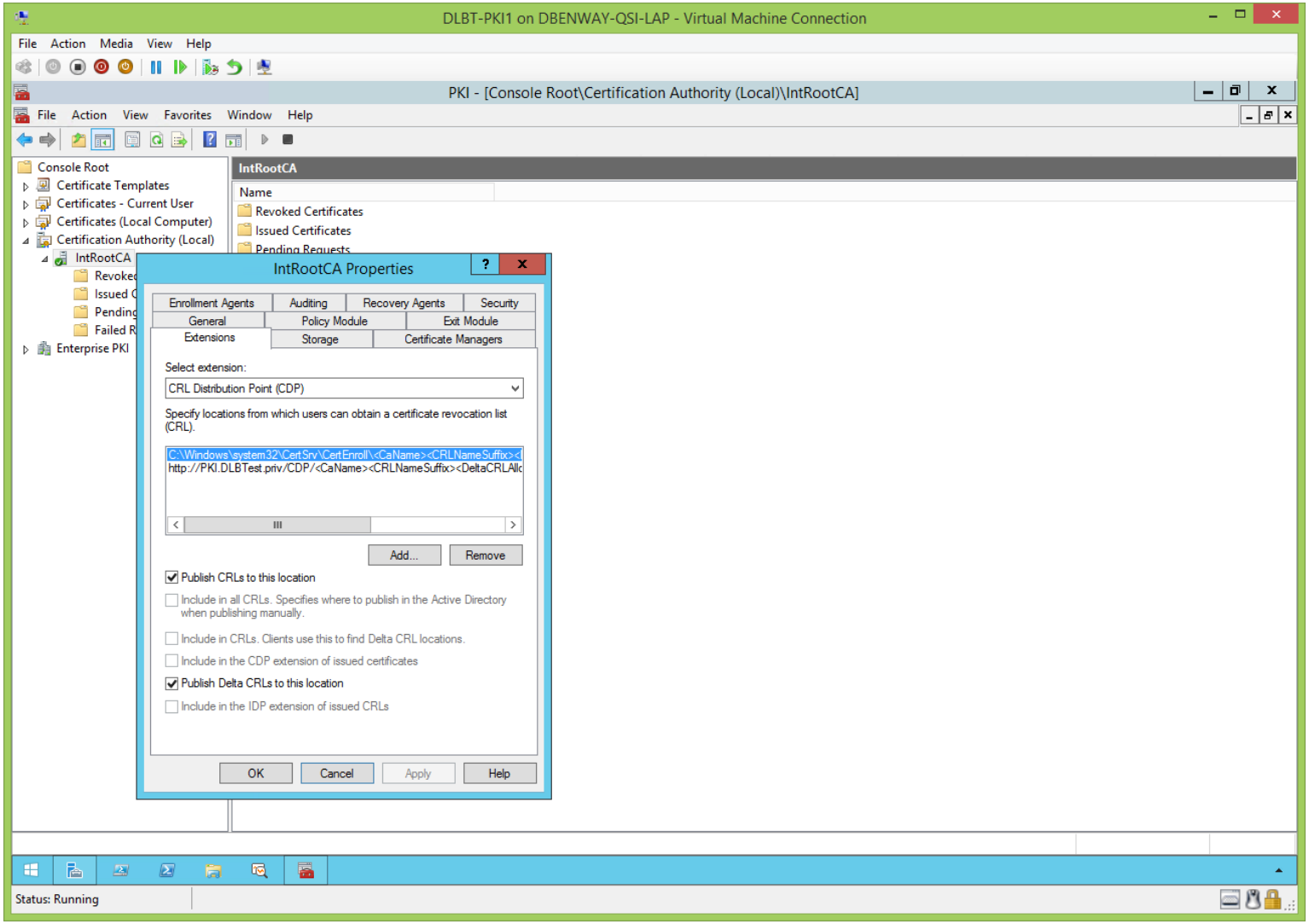
(jump to TOC)

The root CA can't use this, nor can it see templates, because it's not an Enterprise CA.

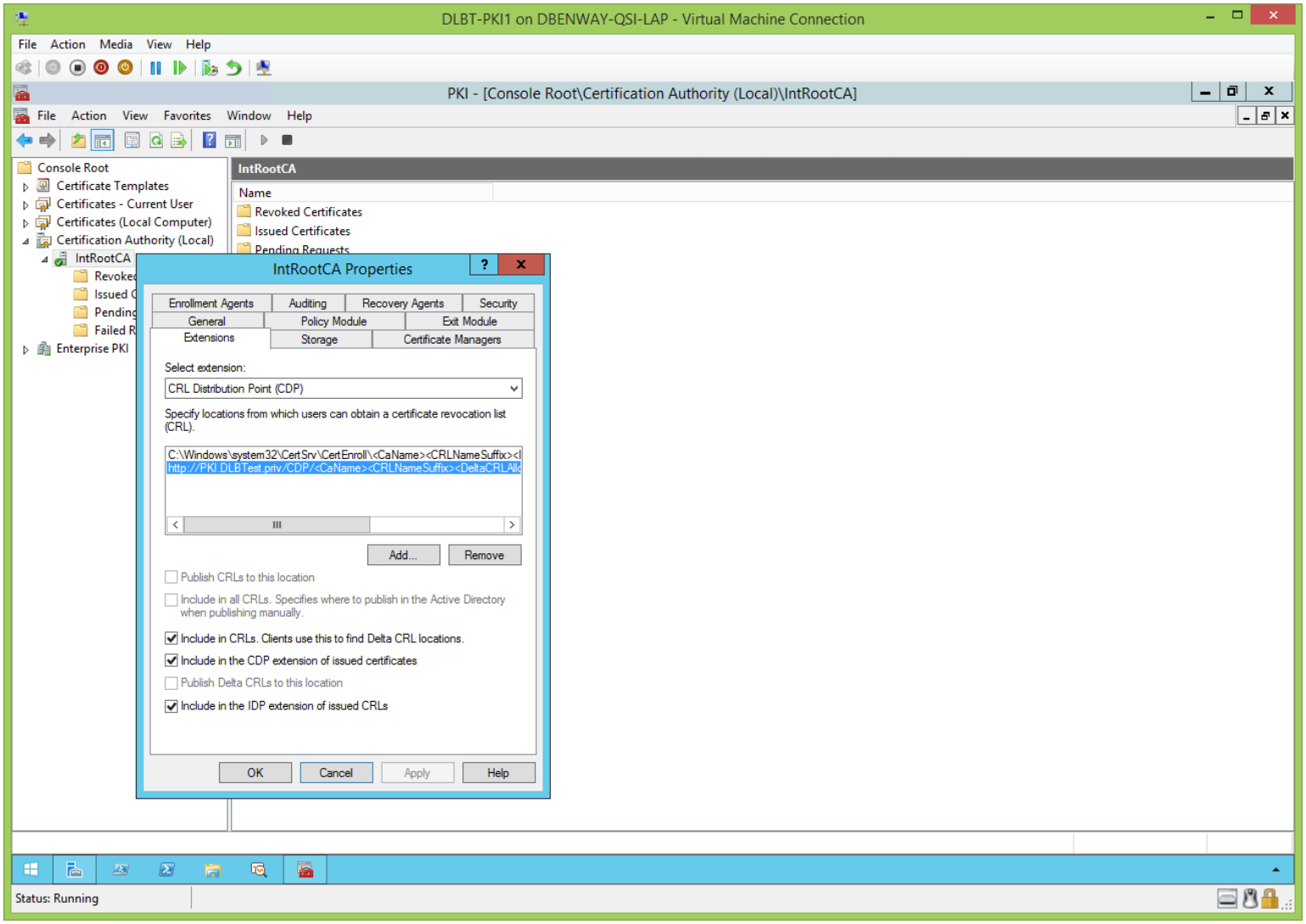
Root CA's Extensions (After CertUtil.exe):

(jump to TOC)

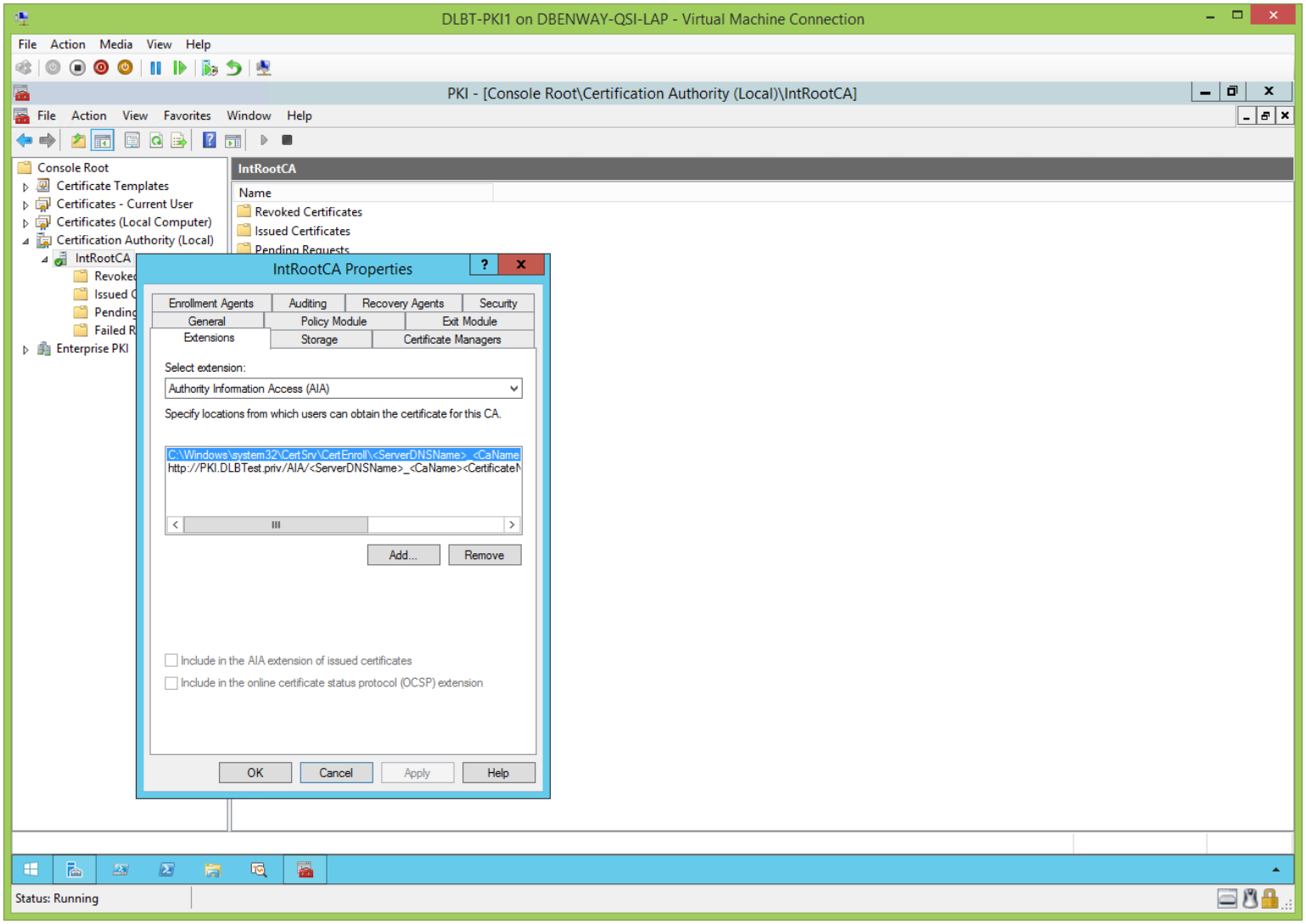
We see now that the root CA's CDP and AIA extensions have been updated by the CertUtil.exe commands:



View the root CA's extensions, cont'd:

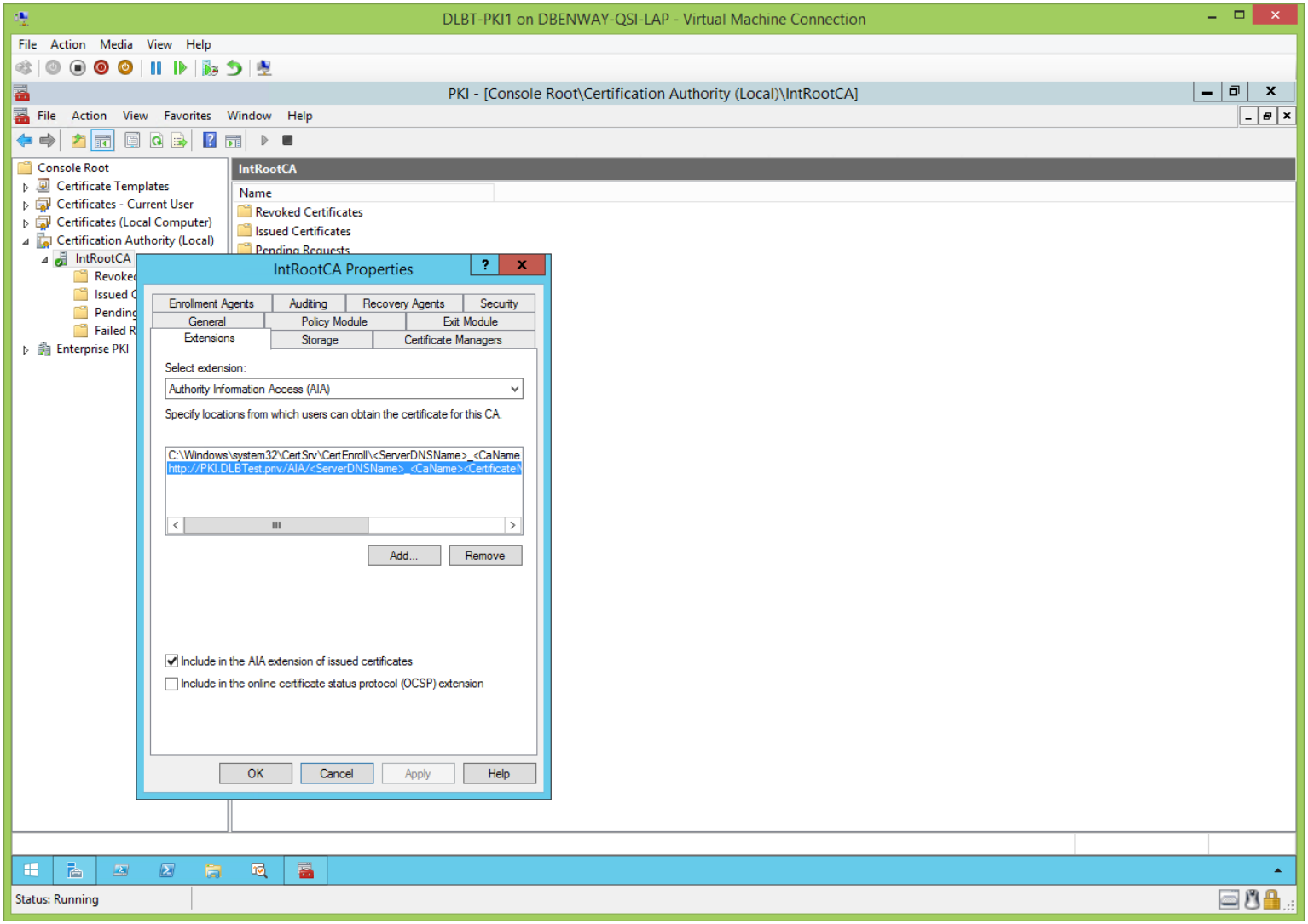


View the root CA's extensions, cont'd:



Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's certificate filename contains the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

View the root CA's extensions, cont'd:

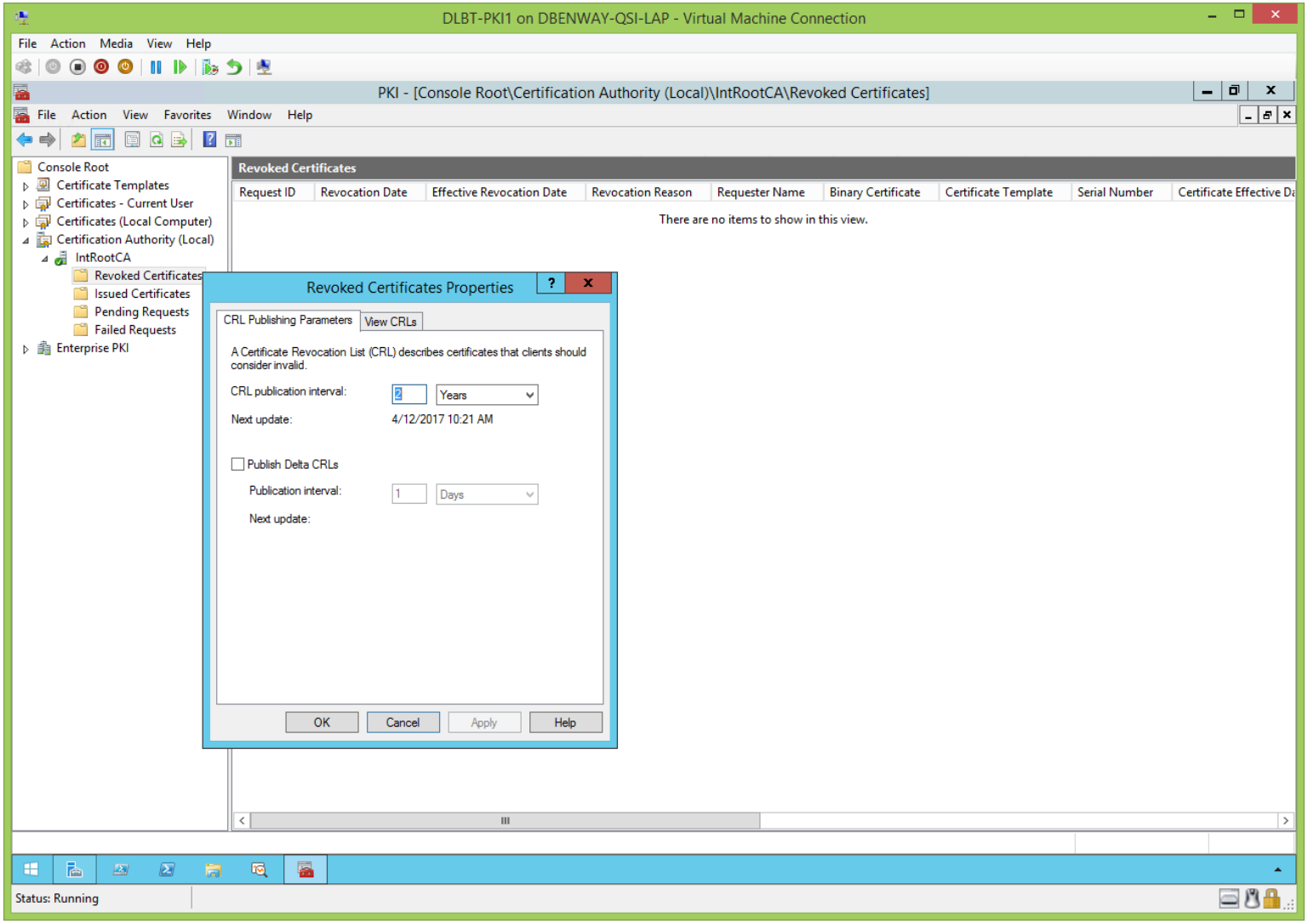


Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's certificate filename contains the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

Root CA's CRLs (After CertUtil.exe):

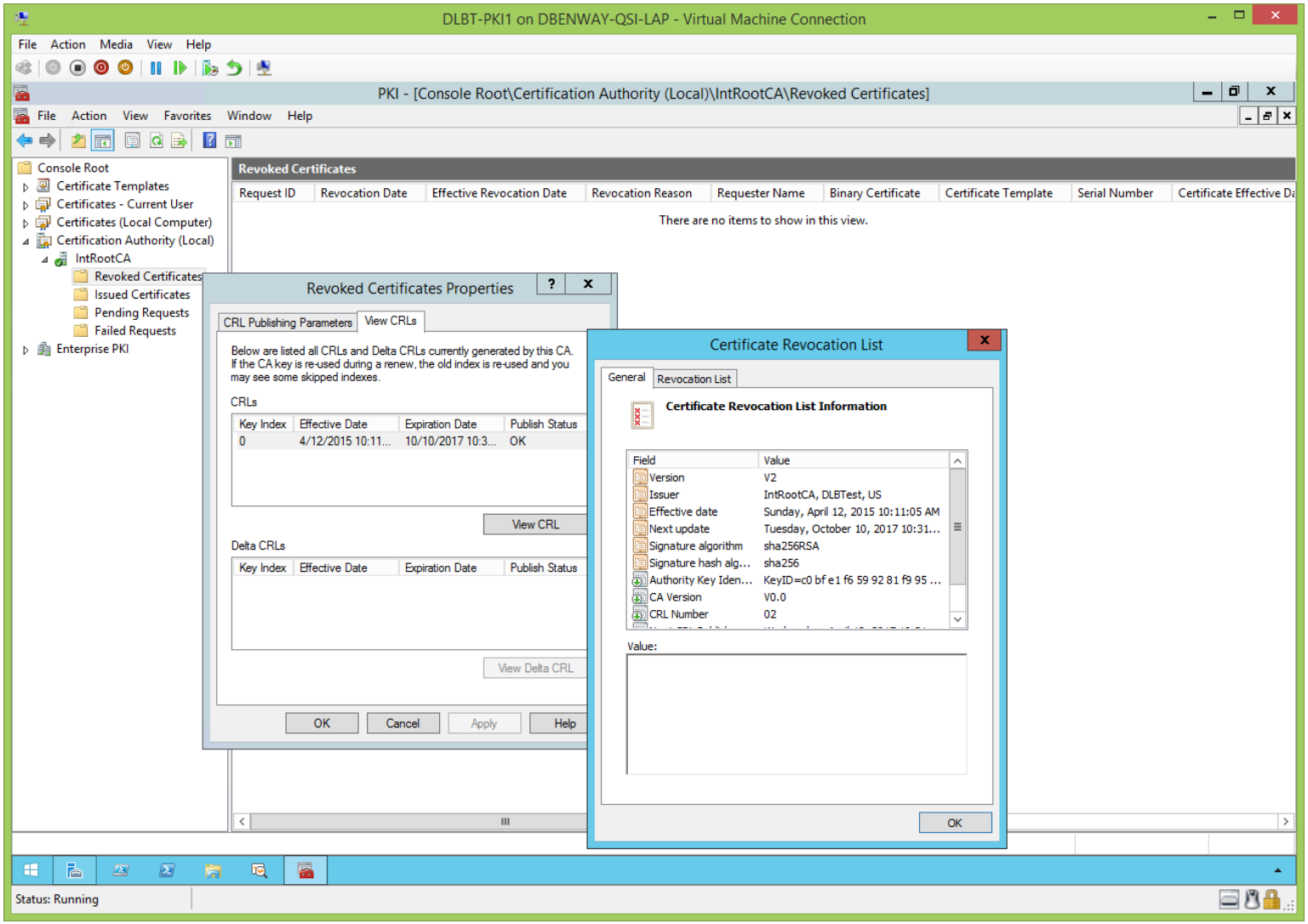
(jump to TOC)

We also see that the root CA's CRL parameters have been updated by the CertUtil.exe commands:

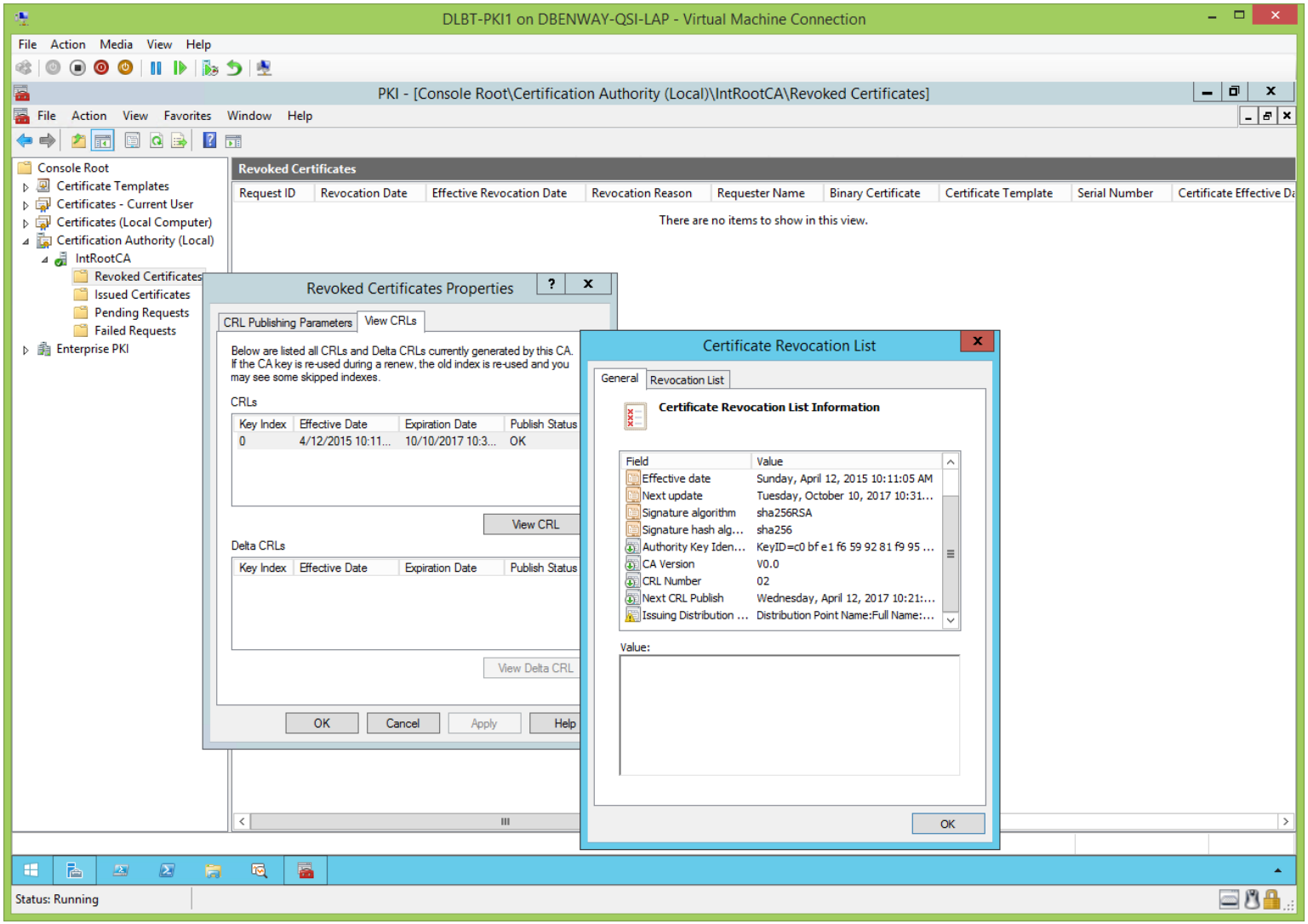


Note: the CertUtil.exe command specified that delta CRLs not be used (0 days) and we see that above (the checkbox is cleared).

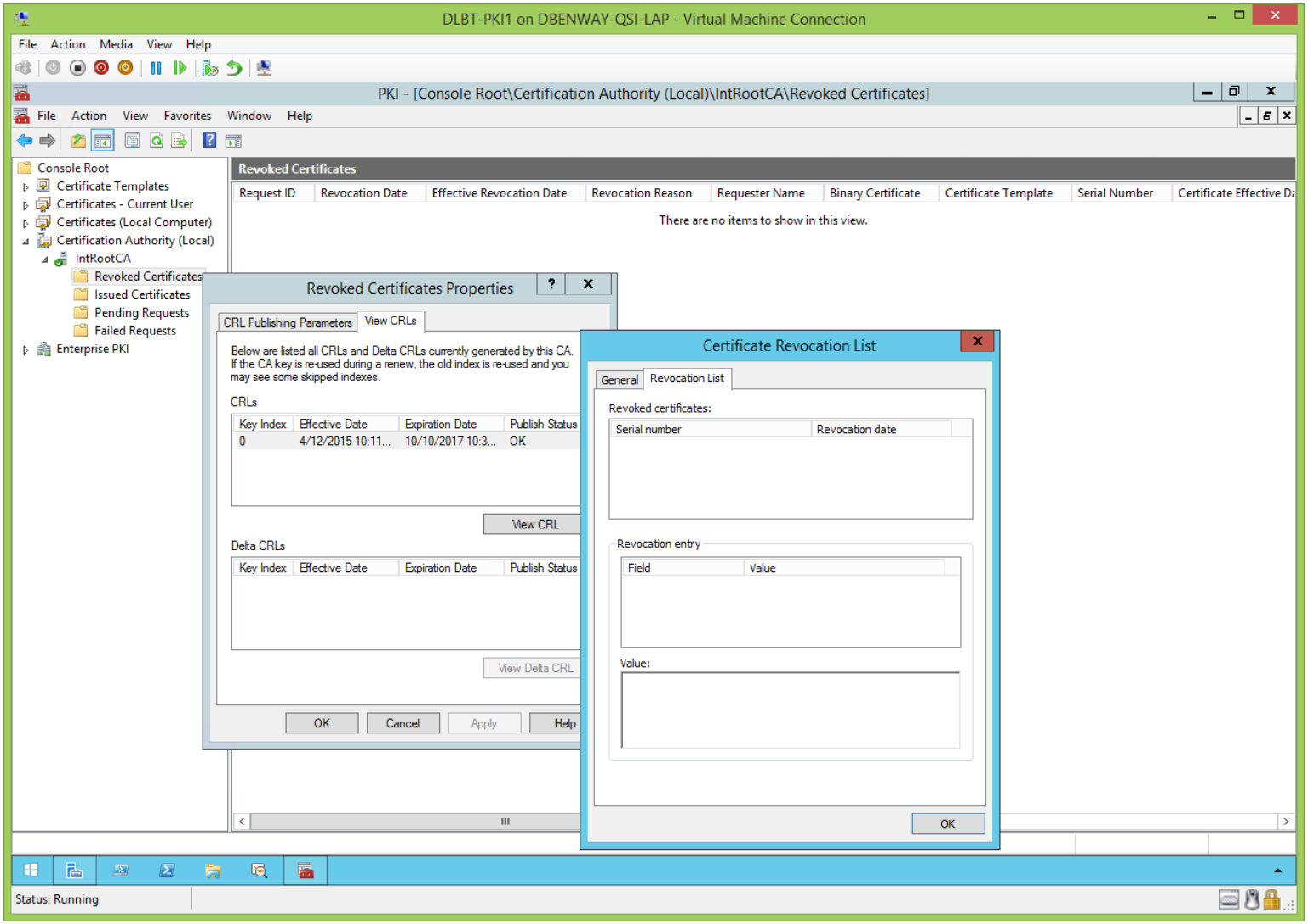
We see that the root CA's CRL has been updated by the CertUtil.exe commands:



View root CA's CRL, cont'd:



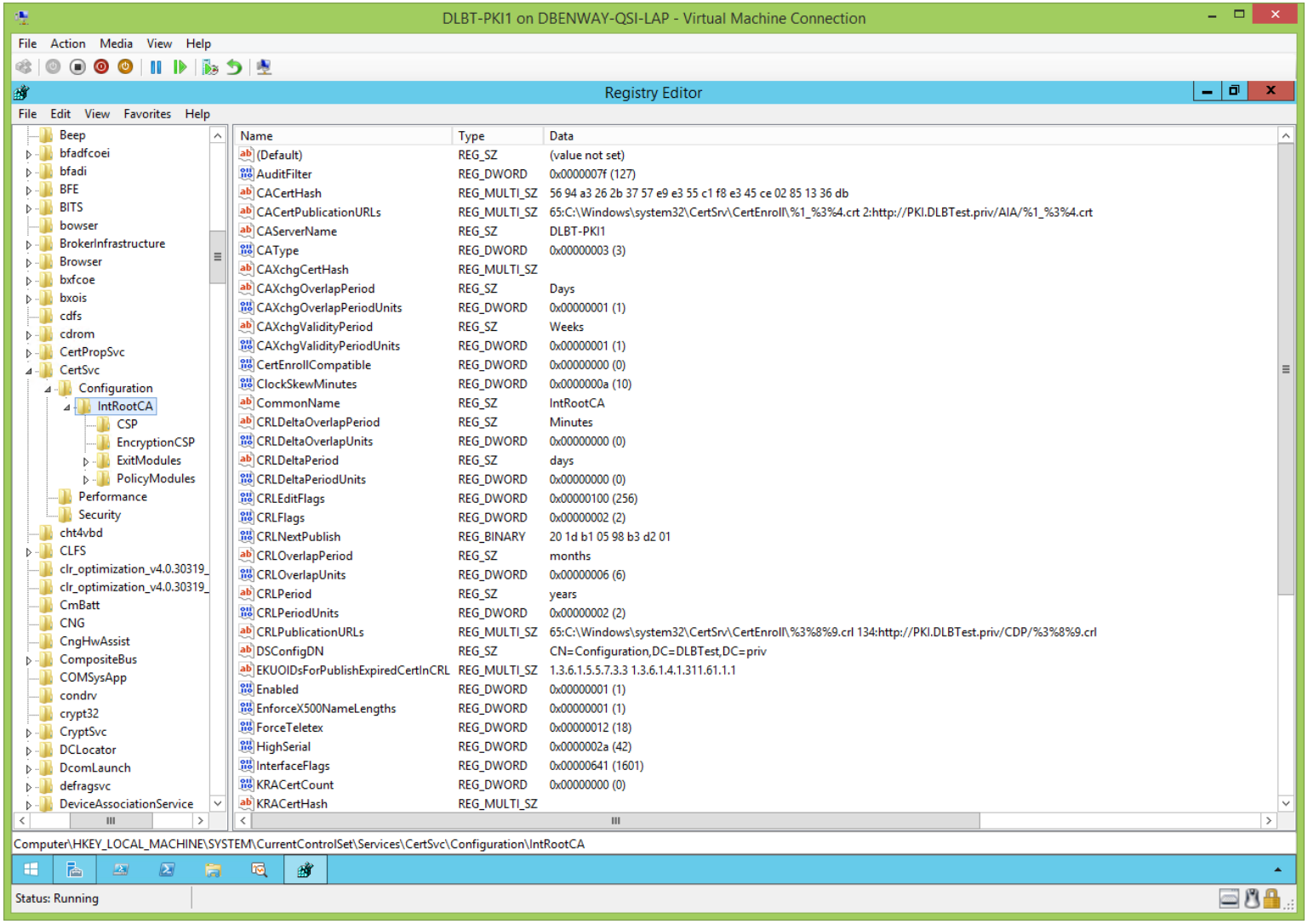
View root CA's CRL, cont'd:



Root CA's Registry (After CertUtil.exe):

(jump to TOC)

We see that the Registry of the root CA has been updated:



Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's certificate filename contains the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

View root CA's Registry, cont'd:

DLBT-PKI1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

Registry Editor

File Edit View Favorites Help

Beep
bfadfcoei
bfadi
BFE
BITS
bowser
BrokerInfrastructure
Browser
bxfcoe
bxois
cdfs
cdrom
CertPropSvc
CertSvc
Configuration
IntRootCA
CSP
EncryptionCSP
ExitModules
PolicyModules
Performance
Security
cht4vbd
CLFS
clr_optimization_v4.0.30319_
clr_optimization_v4.0.30319_
CmBatt
CNG
CngHwAssist
CompositeBus
COMSysApp
condrv
crypt32
CryptSvc
DCLocator
DcomLaunch
defragsvc
DeviceAssociationService

Name	Type	Data
CRLDeltaOverlapUnits	REG_DWORD	0x00000000 (0)
CRLDeltaPeriod	REG_SZ	days
CRLDeltaPeriodUnits	REG_DWORD	0x00000000 (0)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	20 1d b1 05 98 b3 d2 01
CRLOverlapPeriod	REG_SZ	months
CRLOverlapUnits	REG_DWORD	0x00000006 (6)
CRLPeriod	REG_SZ	years
CRLPeriodUnits	REG_DWORD	0x00000002 (2)
CRLPublicationURLs	REG_MULTI_SZ	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl 134:http://PKI.DLBTest.priv/CDP/%3%8%9.crl
DSConfigDN	REG_SZ	CN=Configuration,DC=DLBTest,DC=priv
EKUOIDsForPublishExpiredCertInCRL	REG_MULTI_SZ	1.3.6.1.5.5.7.3.3 1.3.6.1.4.1.311.61.1.1
Enabled	REG_DWORD	0x00000001 (1)
EnforceX500NameLengths	REG_DWORD	0x00000001 (1)
ForceTeletex	REG_DWORD	0x00000012 (18)
HighSerial	REG_DWORD	0x0000002a (42)
InterfaceFlags	REG_DWORD	0x00000641 (1601)
KRACertCount	REG_DWORD	0x00000000 (0)
KRACertHash	REG_MULTI_SZ	
KRAFlags	REG_DWORD	0x00000000 (0)
LogLevel	REG_DWORD	0x00000003 (3)
MaxIncomingAllocSize	REG_DWORD	0x00010000 (65536)
MaxIncomingMessageSize	REG_DWORD	0x00010000 (65536)
PolicyFlags	REG_DWORD	0x00000000 (0)
Security	REG_BINARY	01 00 14 84 90 00 00 00 a0 00 00 00 14 00 00 00 44 00 00 00 02 00 30 00 02 00 00 00 02 c0 14 00 ff ff 00 00 01 01 00 00 00 00 00 01 00 00 00 00 02
SetupStatus	REG_DWORD	0x00000001 (1)
SignedAttributes	REG_MULTI_SZ	RequesterName
SubjectTemplate	REG_MULTI_SZ	EMail CommonName OrganizationalUnit Organization Locality State DomainComponent Country
UseDS	REG_DWORD	0x00000000 (0)
ValidityPeriod	REG_SZ	years
ValidityPeriodUnits	REG_DWORD	0x0000000a (10)
ViewAgeMinutes	REG_DWORD	0x00000010 (16)
ViewIdleMinutes	REG_DWORD	0x00000008 (8)

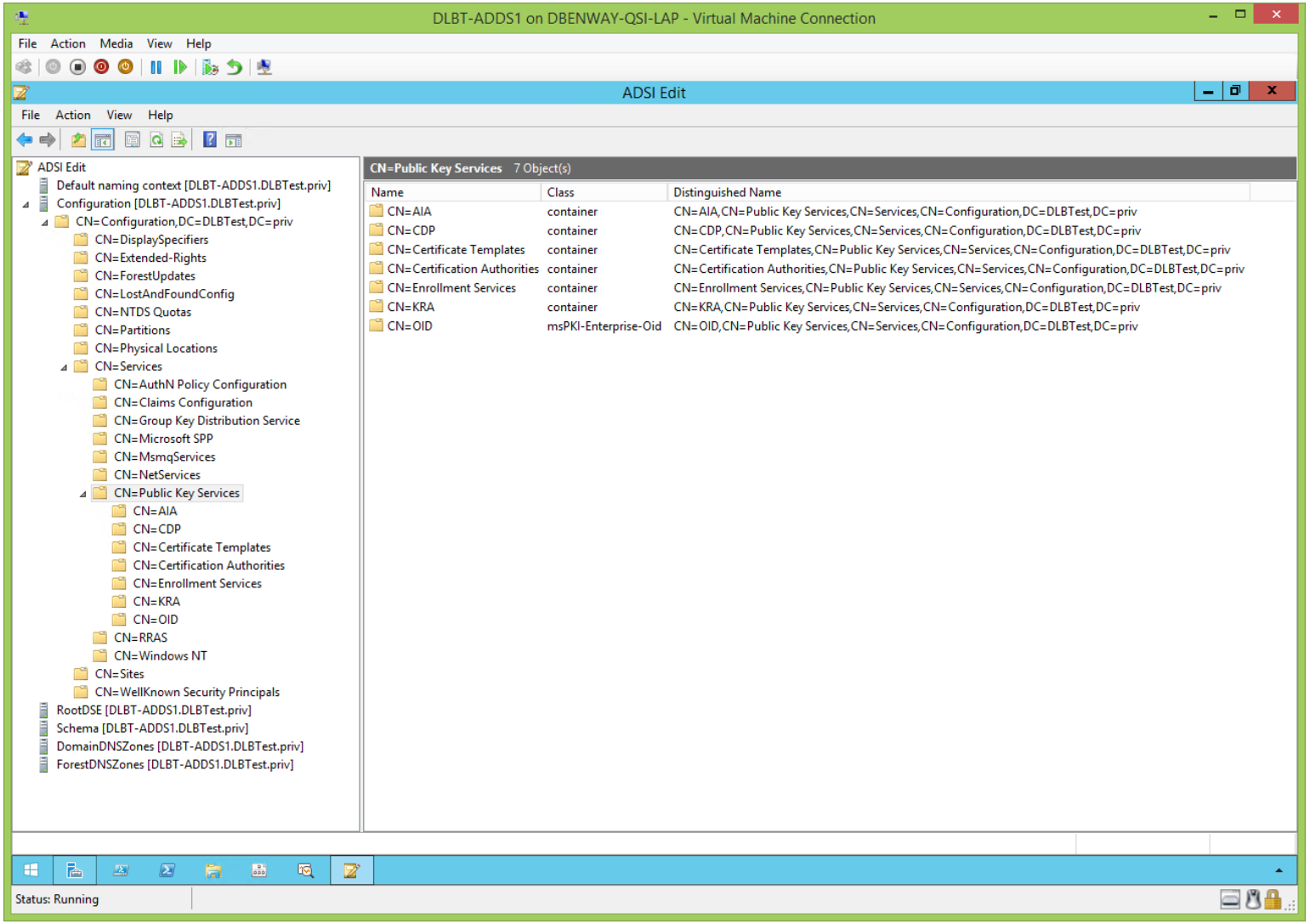
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\IntRootCA

Status: Running

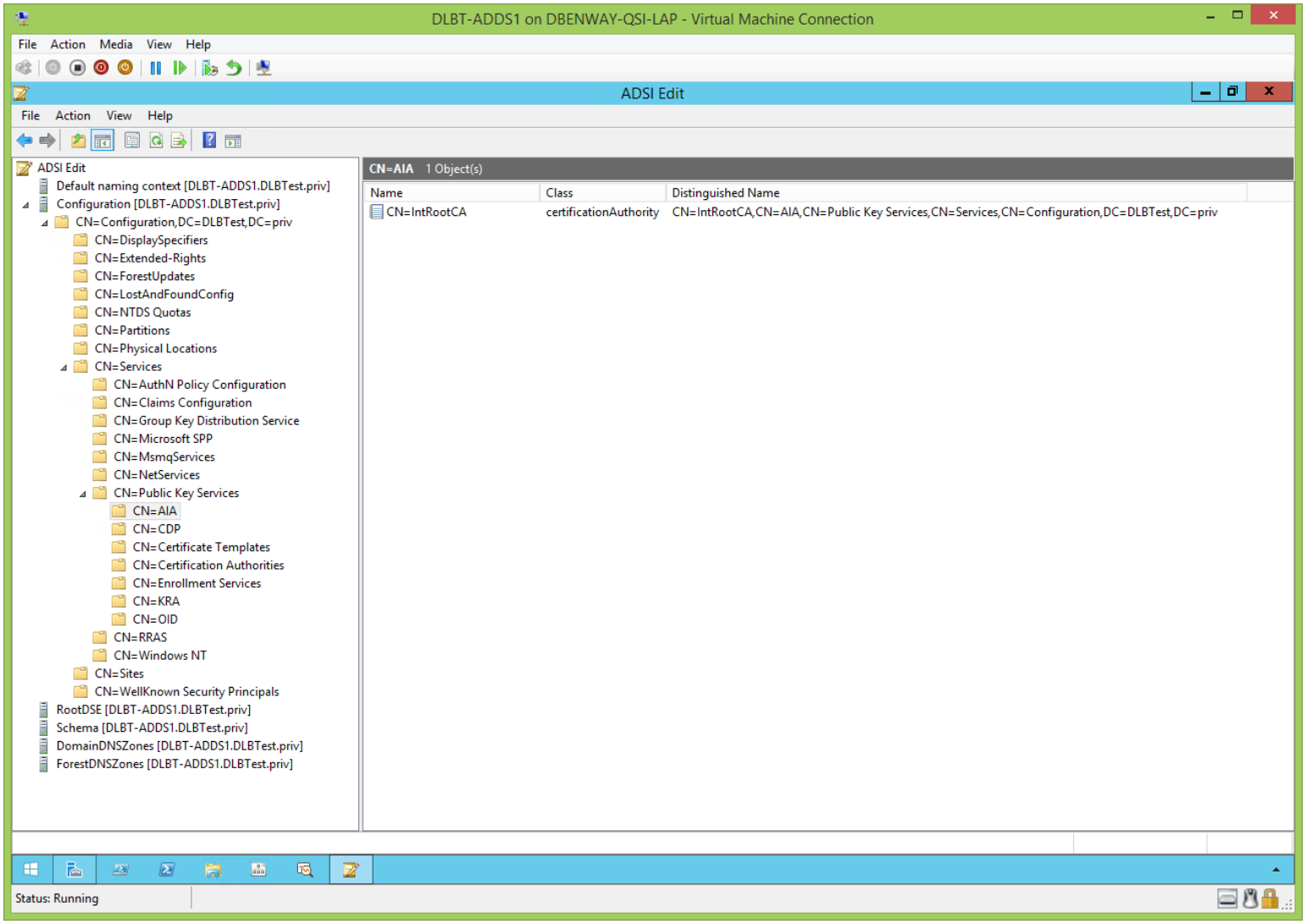
ADSIEdit.msc (After CertUtil.exe):

(jump to TOC)

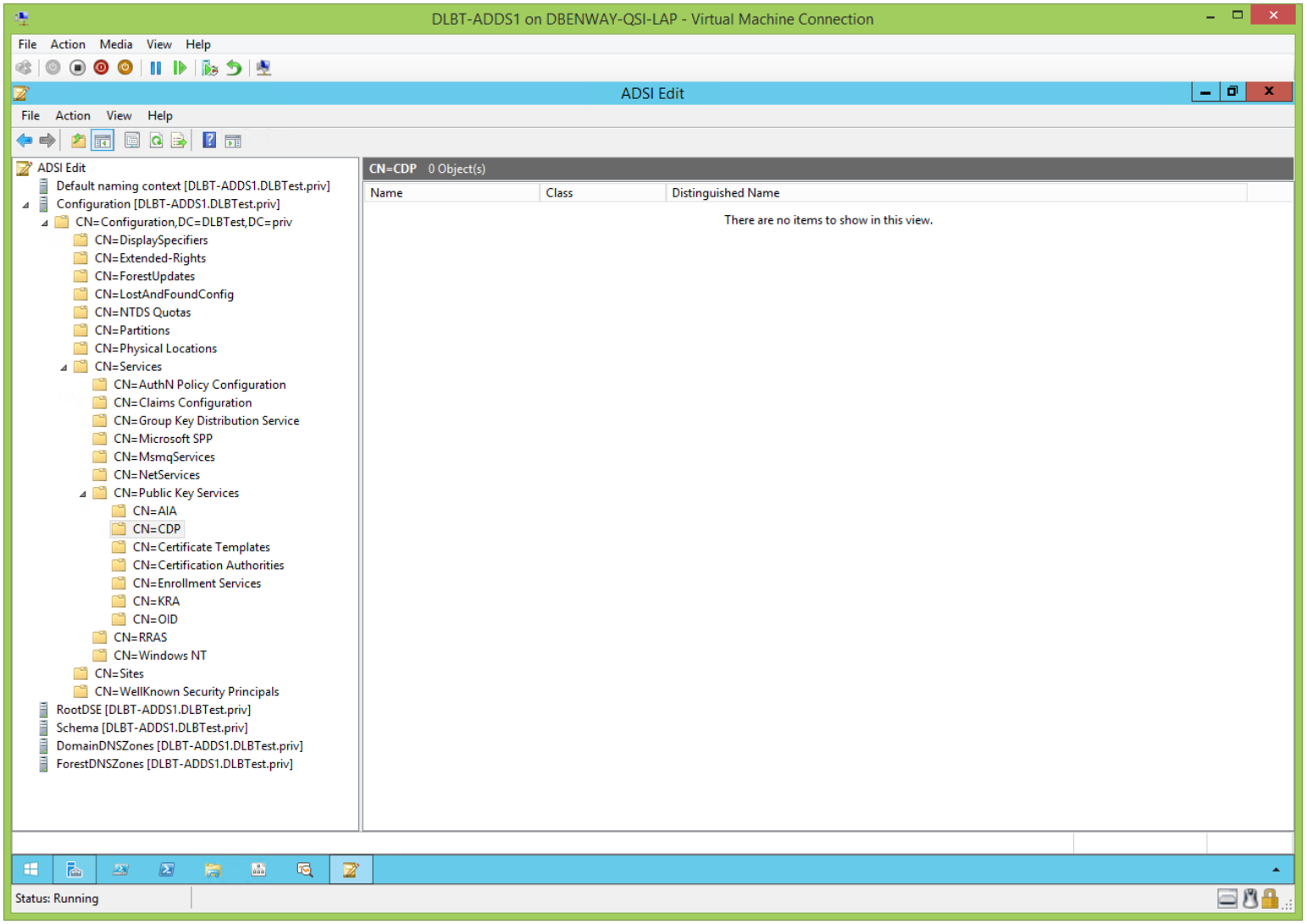
We see the root CA's information has been published to the Active Directory:



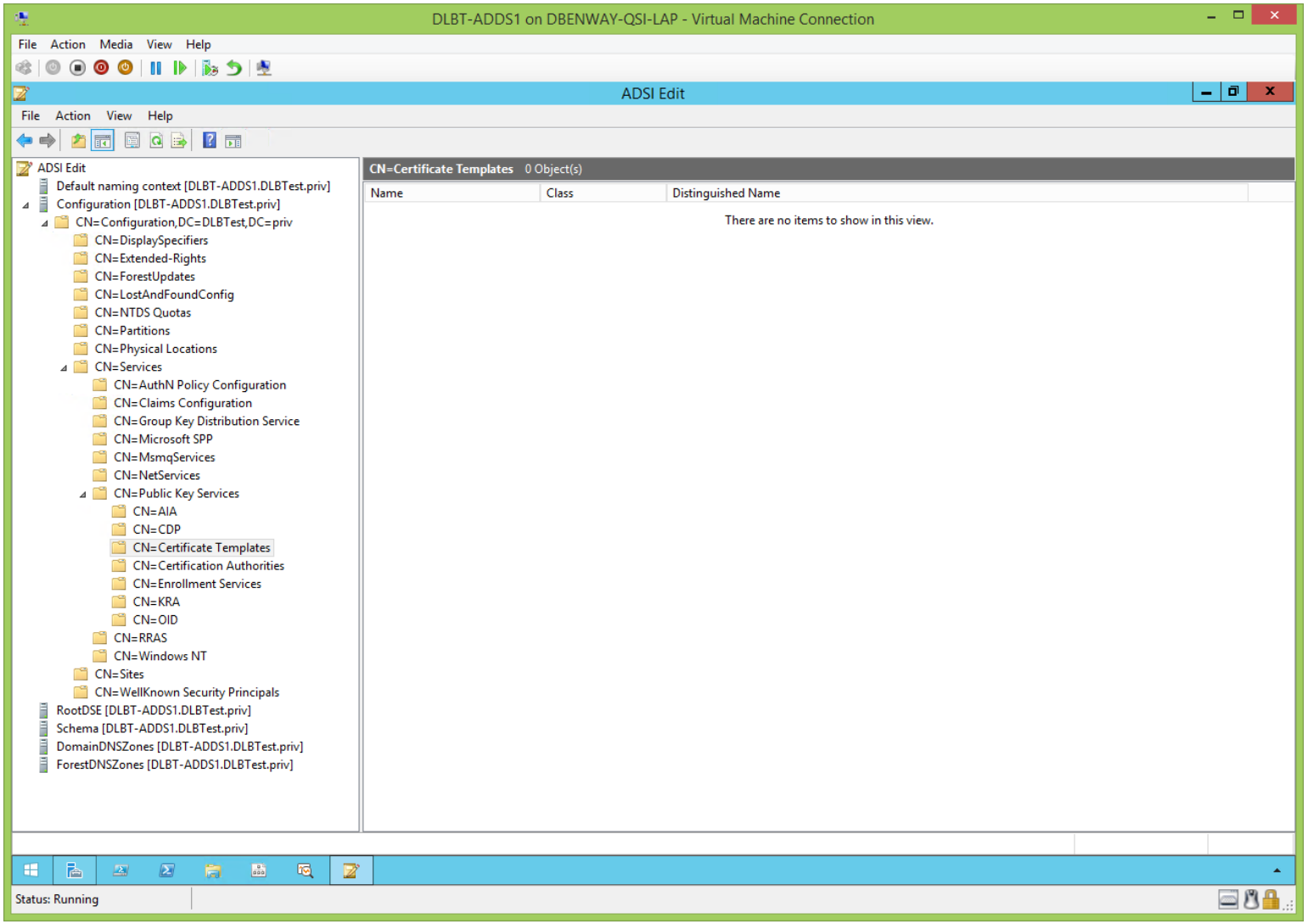
View ADSIEdit.msc, cont'd:



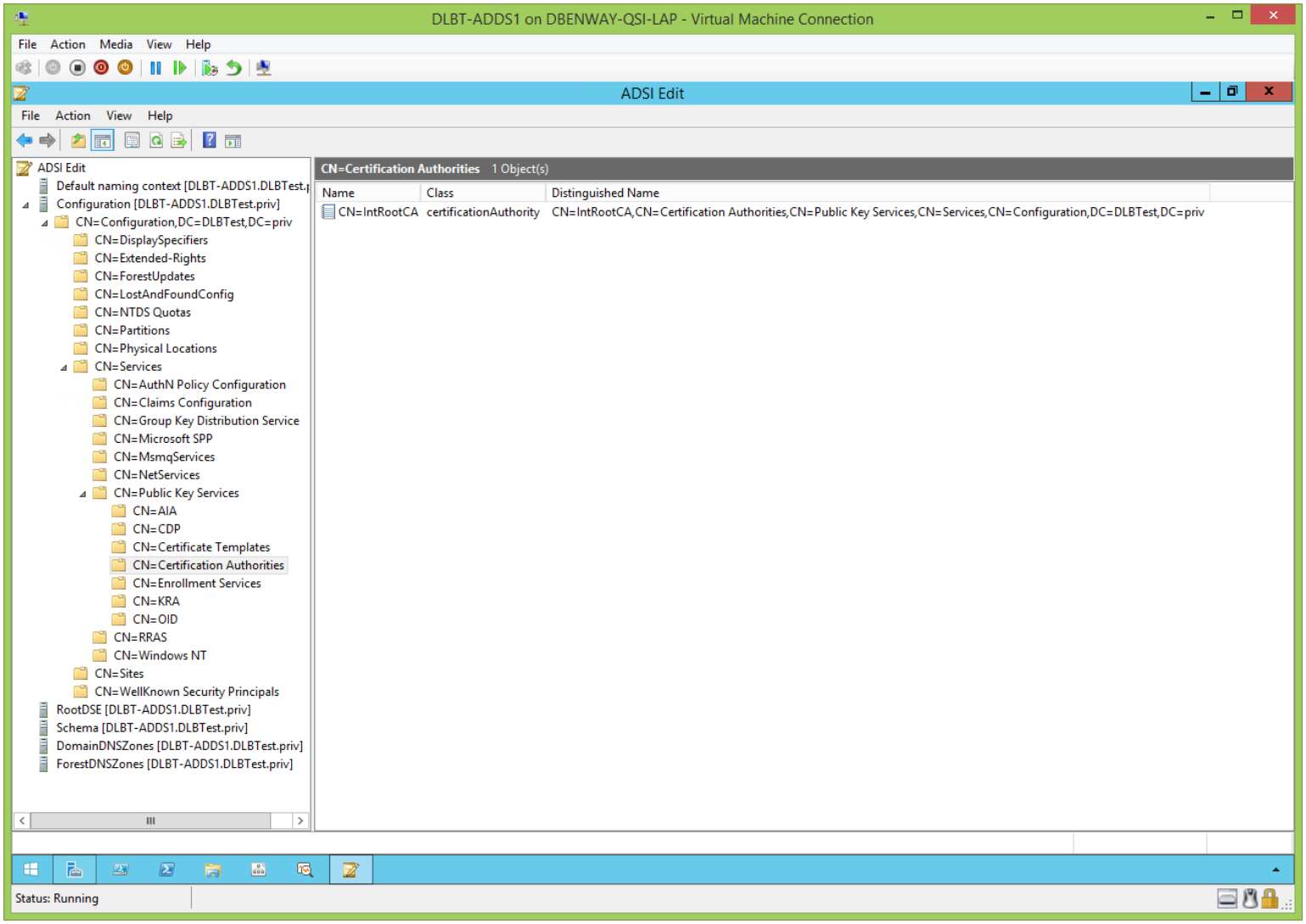
View ADSIEdit.msc, cont'd:



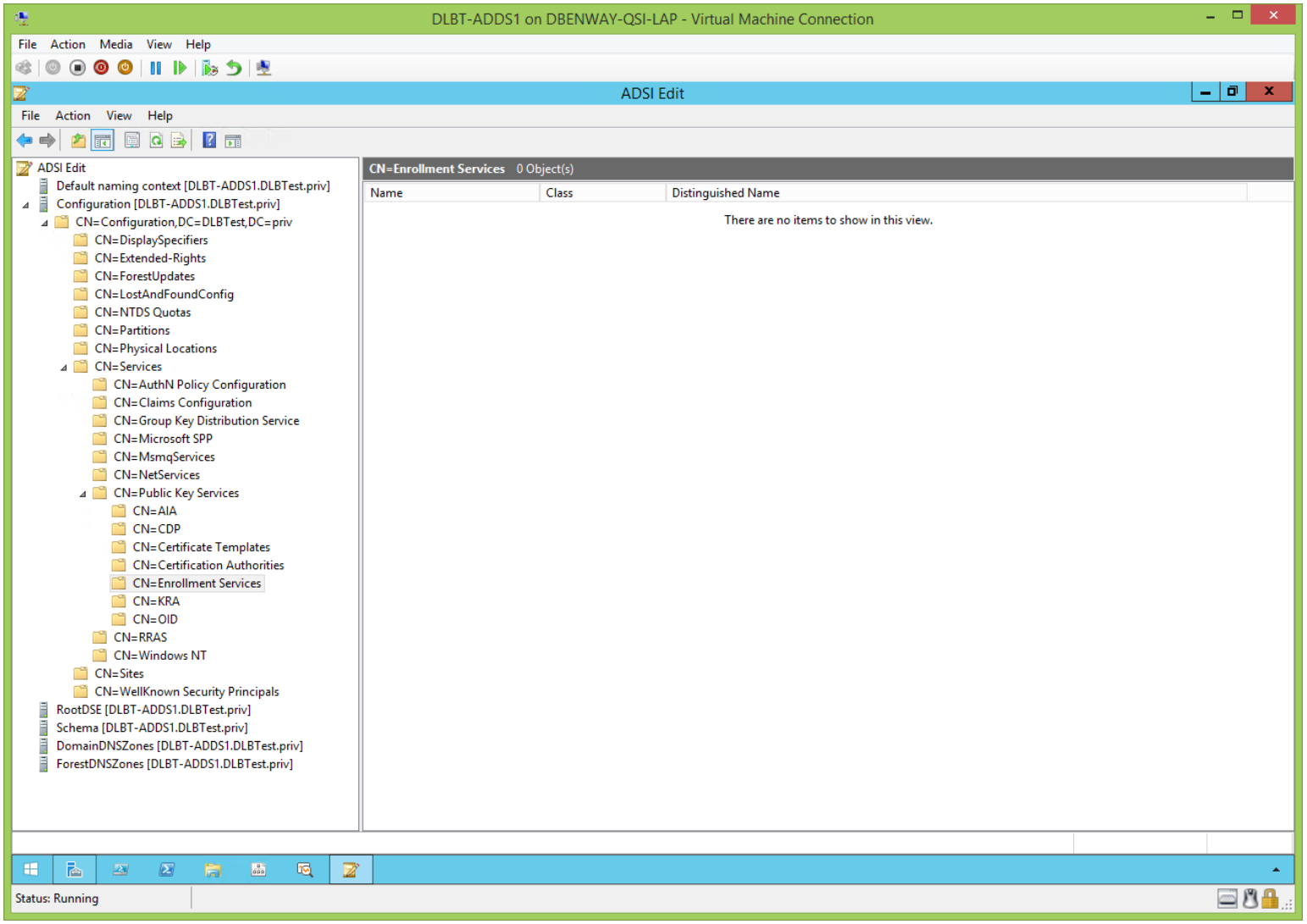
View ADSIEdit.msc, cont'd:



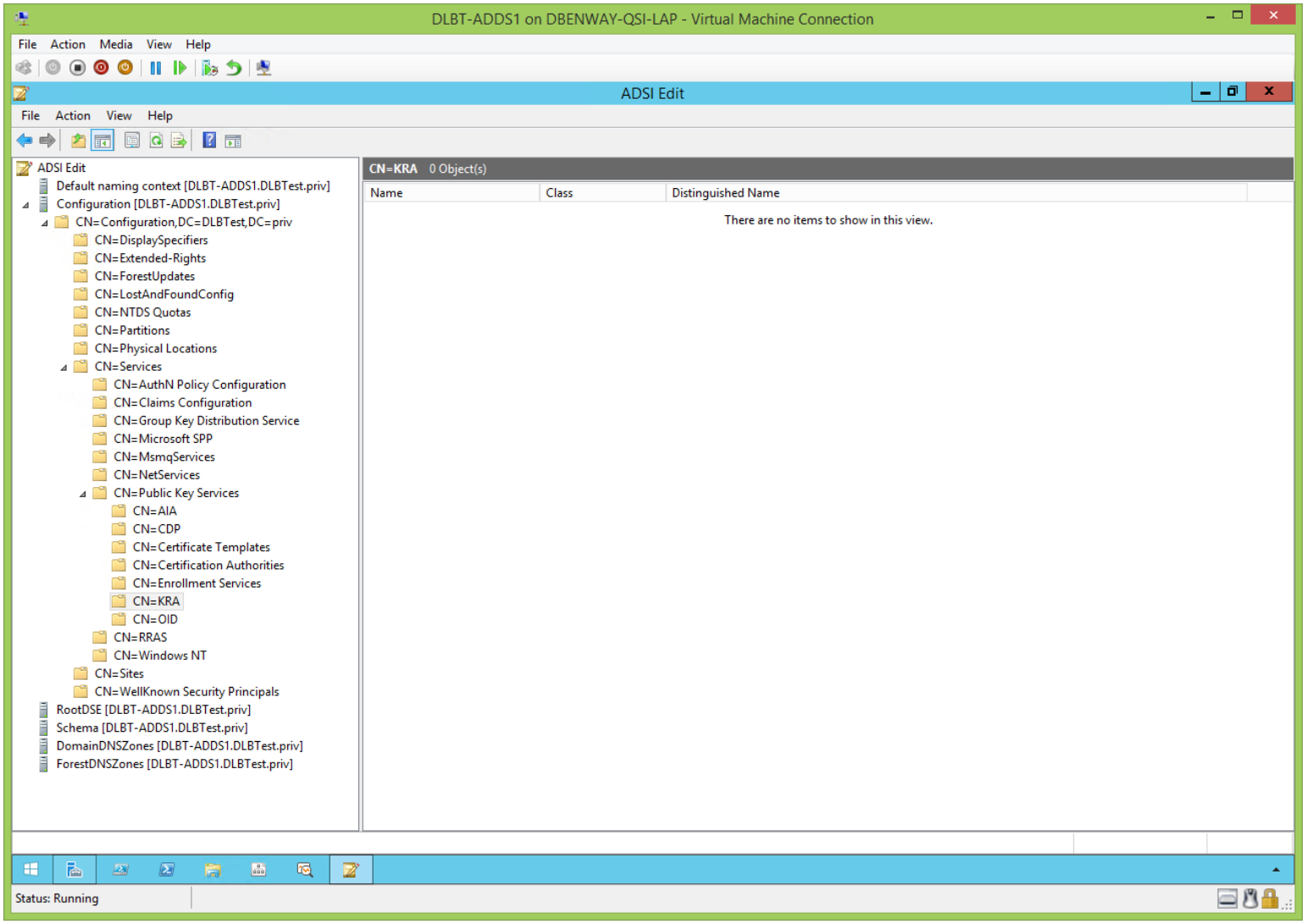
View ADSIEdit.msc, cont'd:



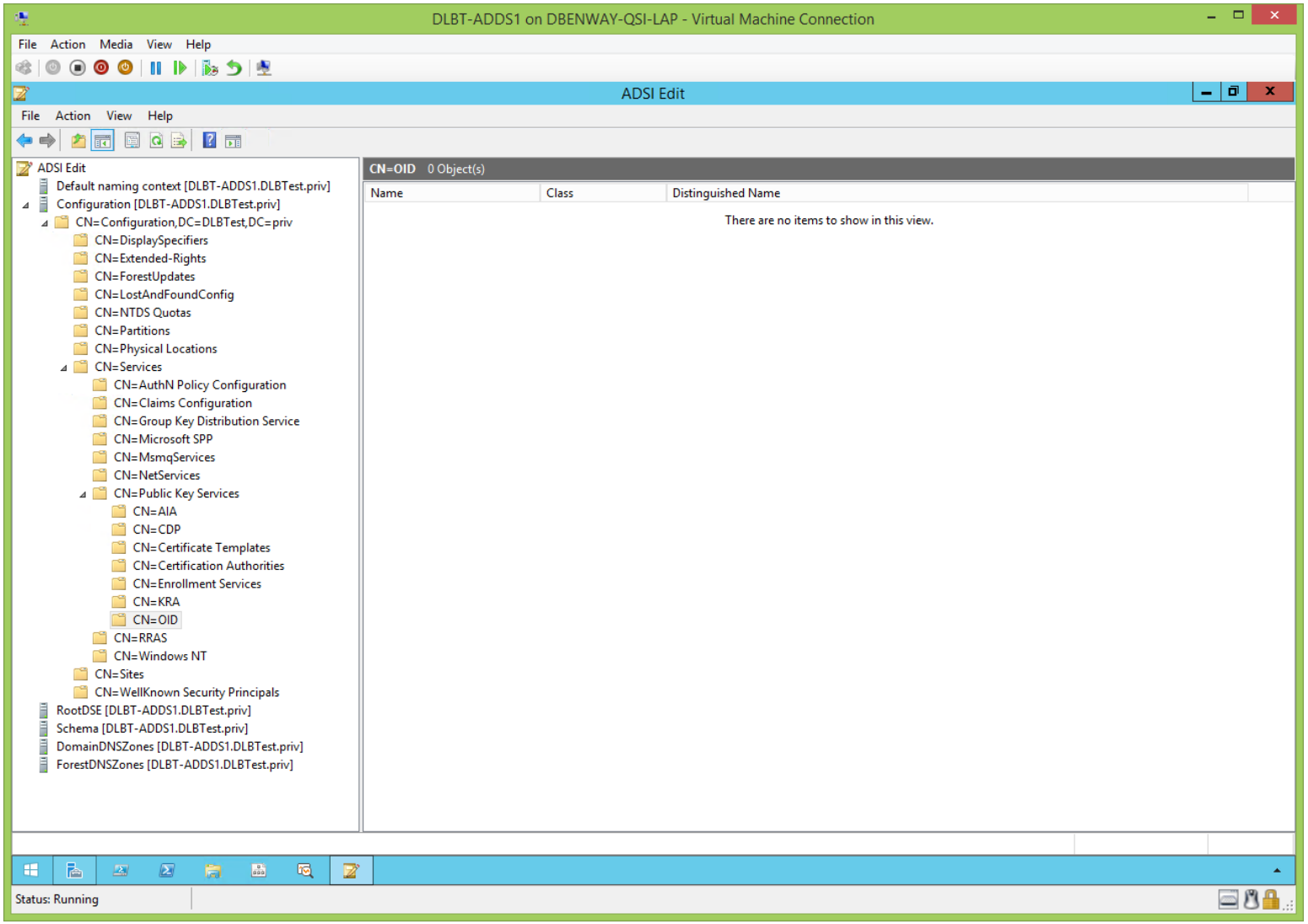
View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:



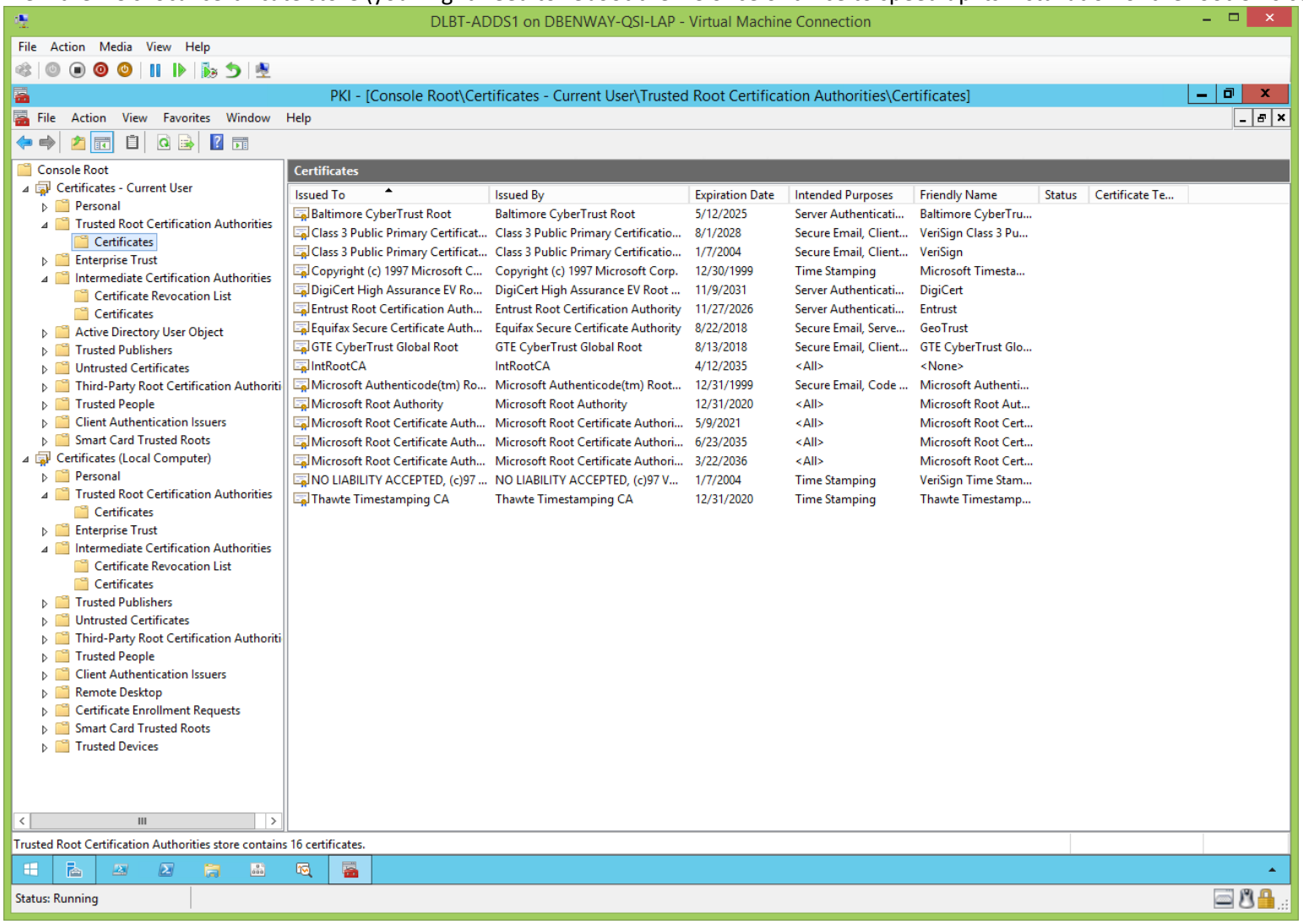
View ADSIEdit.msc, cont'd:



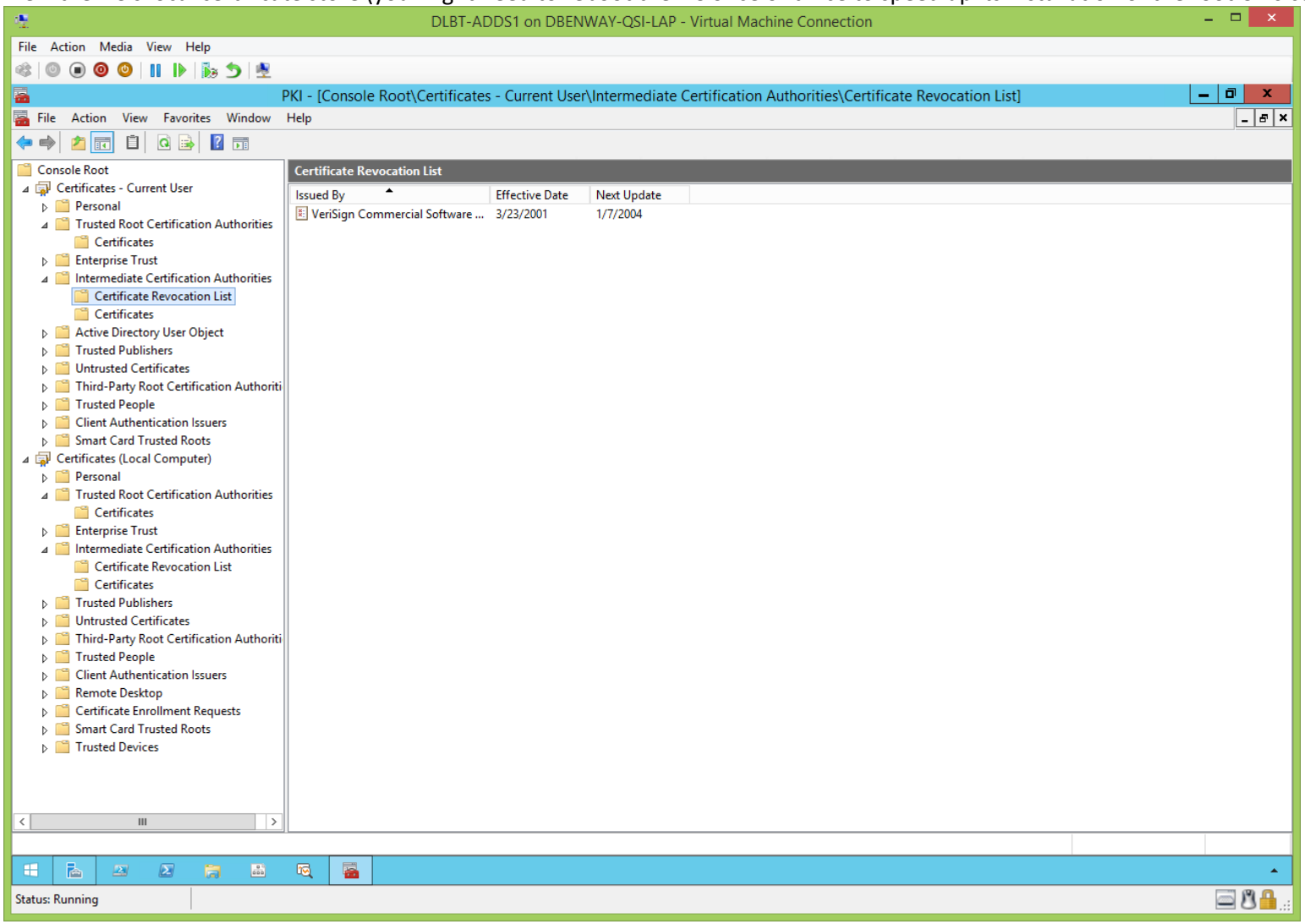
DC's Local Certificate Store (After CertUtil.exe):

(jump to TOC)

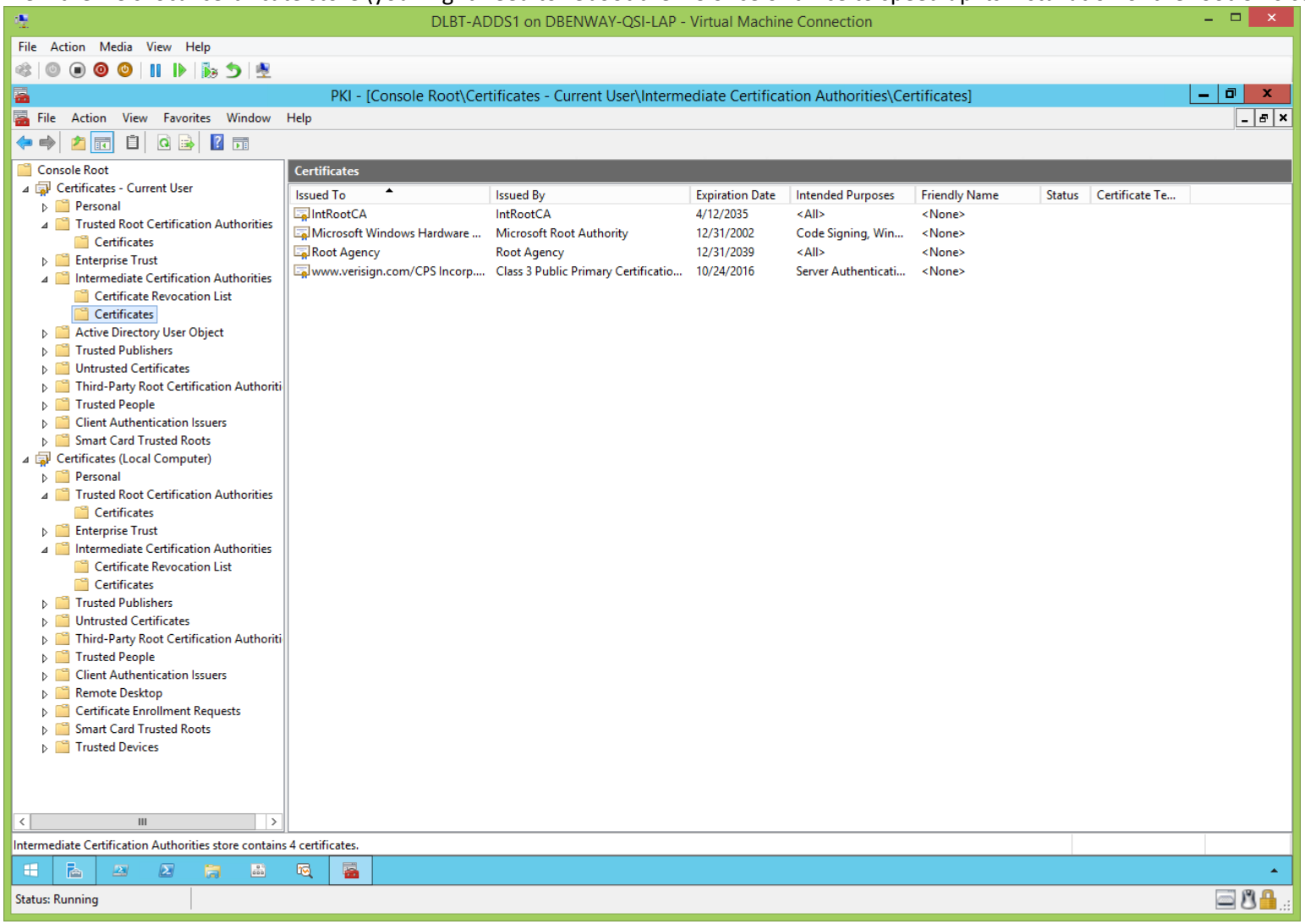
View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the root CA's certificate from AD):



View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the root CA's certificate from AD), cont'd:



View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the root CA's certificate from AD), cont'd:



View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the root CA's certificate from AD), cont'd:

DLBT-ADDS1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

PKI - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authoriti
    - Trusted People
    - Client Authentication Issuers
    - Smart Card Trusted Roots
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authoriti
    - Trusted People
    - Client Authentication Issuers
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices

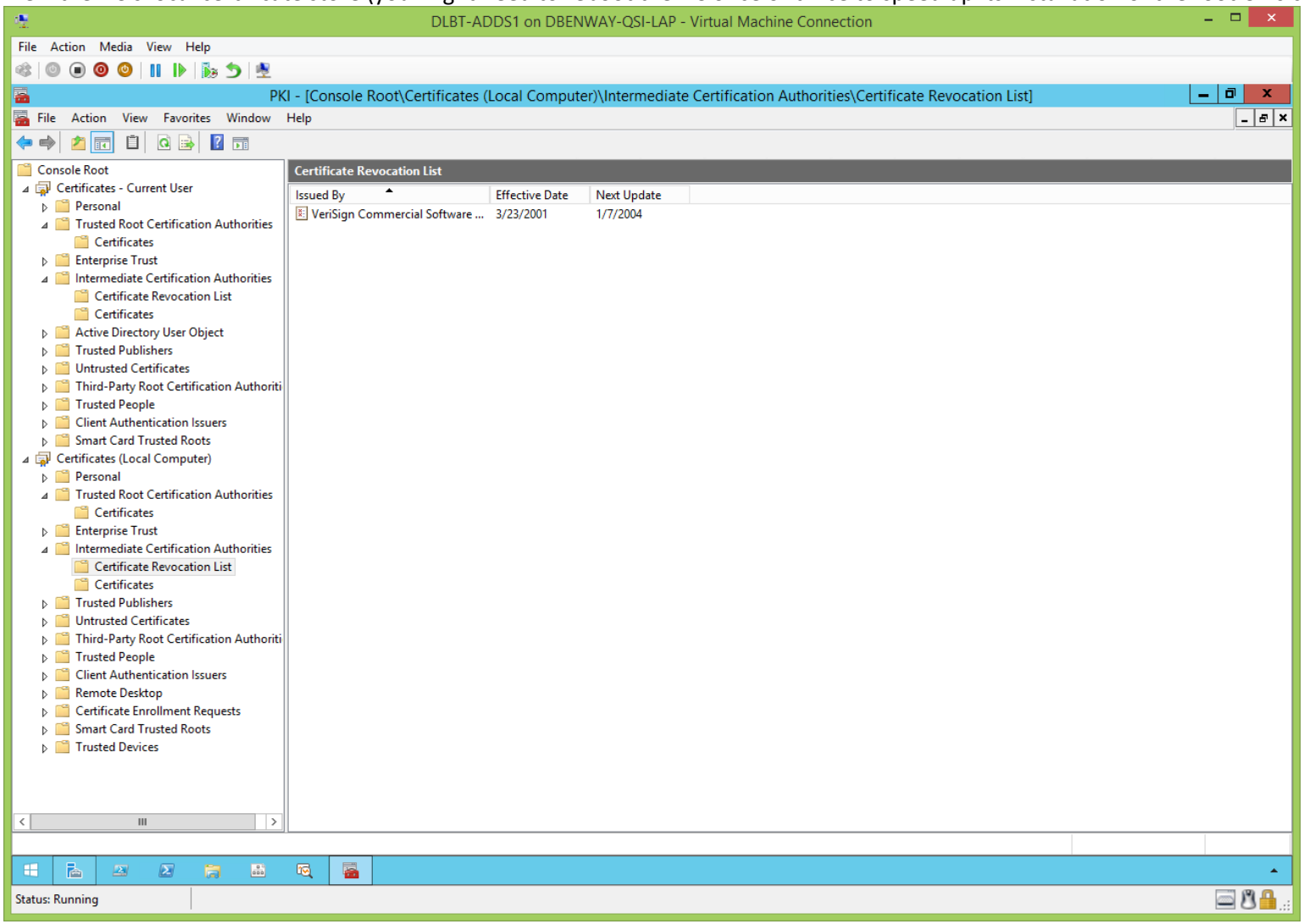
Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	Baltimore CyberTru...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
Entrust Root Certification Auth...	Entrust Root Certification Authority	11/27/2026	Server Authenticati...	Entrust		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...		
IntRootCA	IntRootCA	4/12/2035	<All>	<None>		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		

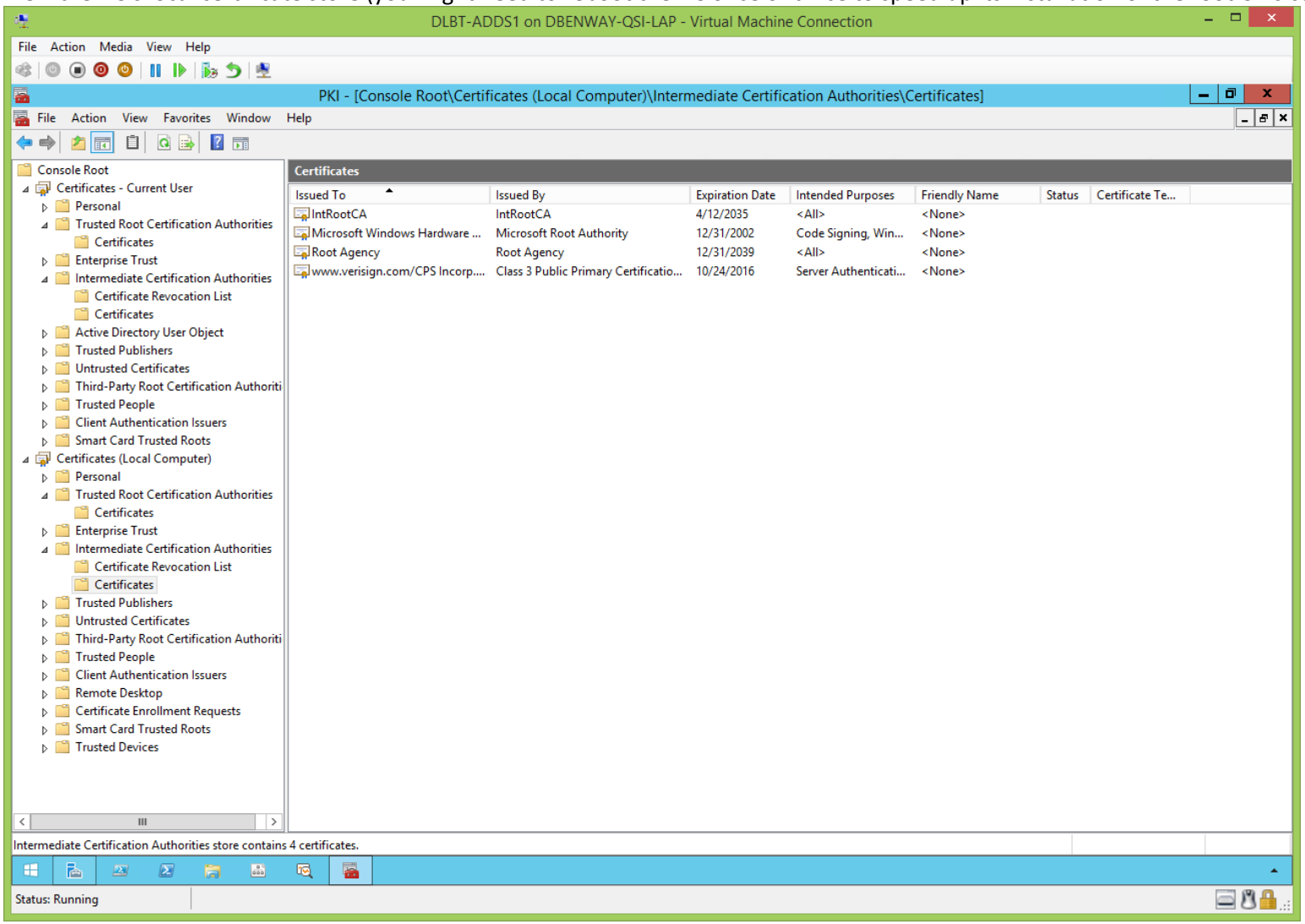
Trusted Root Certification Authorities store contains 16 certificates.

Status: Running

View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the root CA's certificate from AD), cont'd:



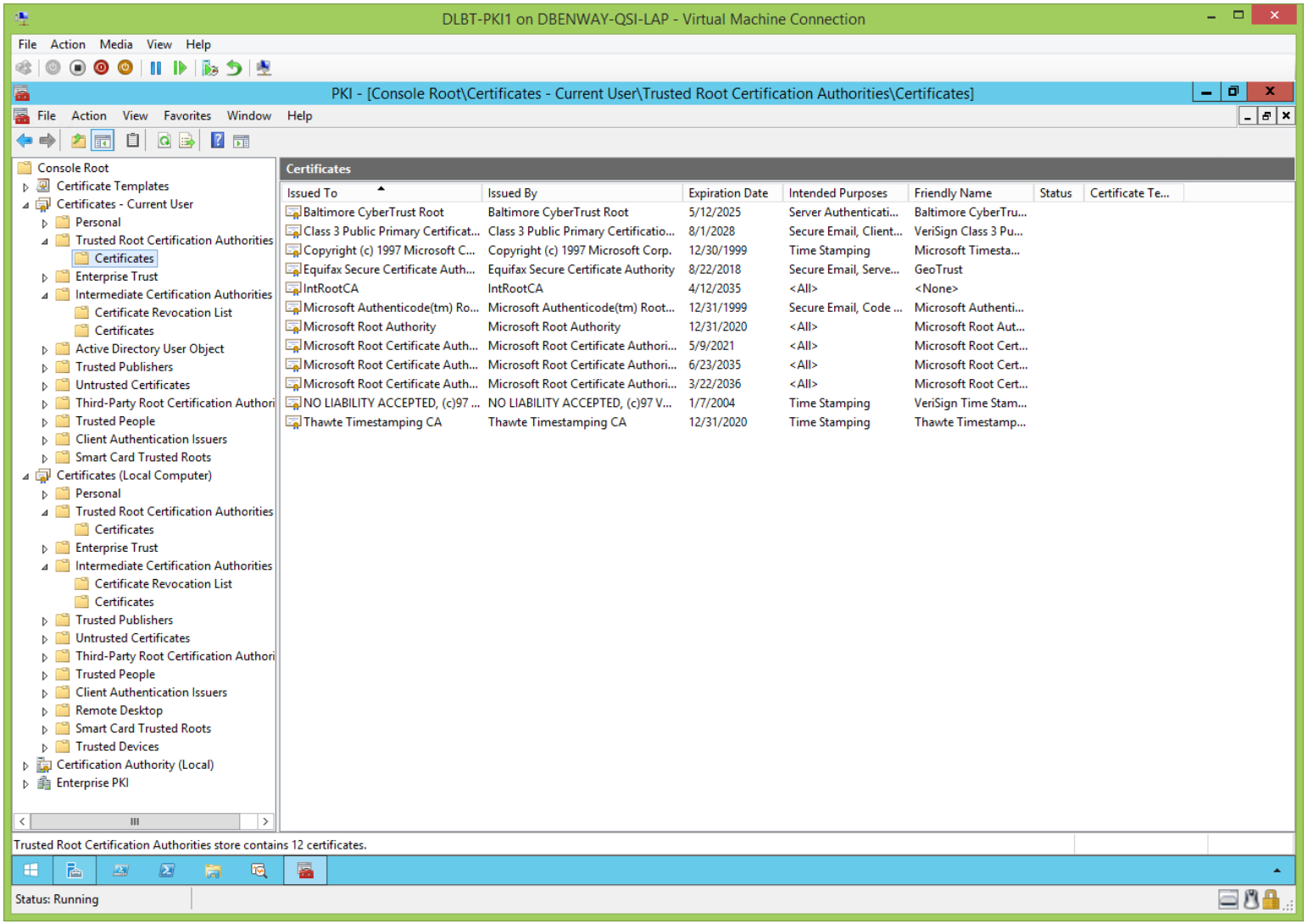
View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the root CA's certificate from AD), cont'd:



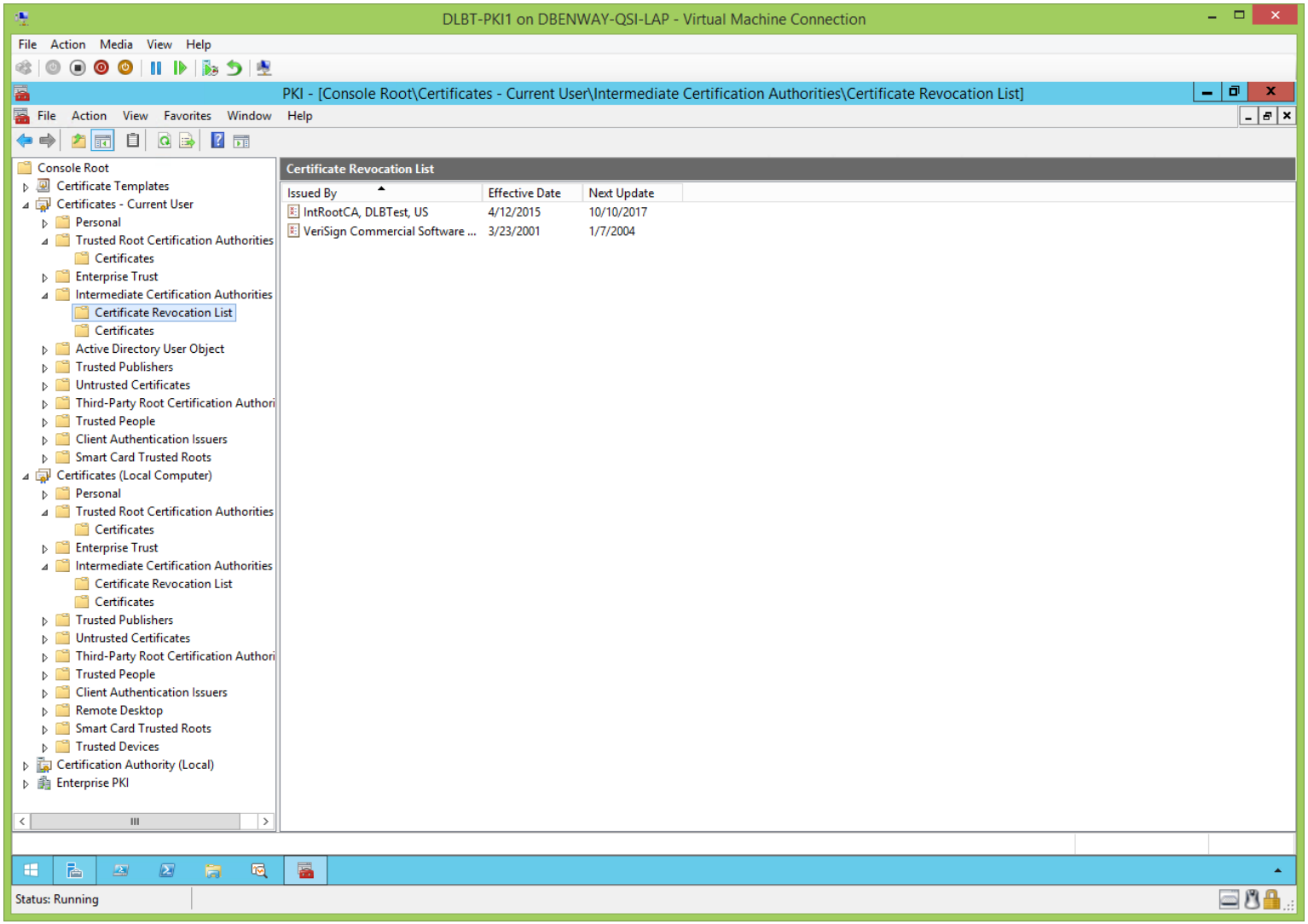
Root CA's Local Certificate Store (After CertUtil.exe):

(jump to TOC)

View root CA's local certificate store:

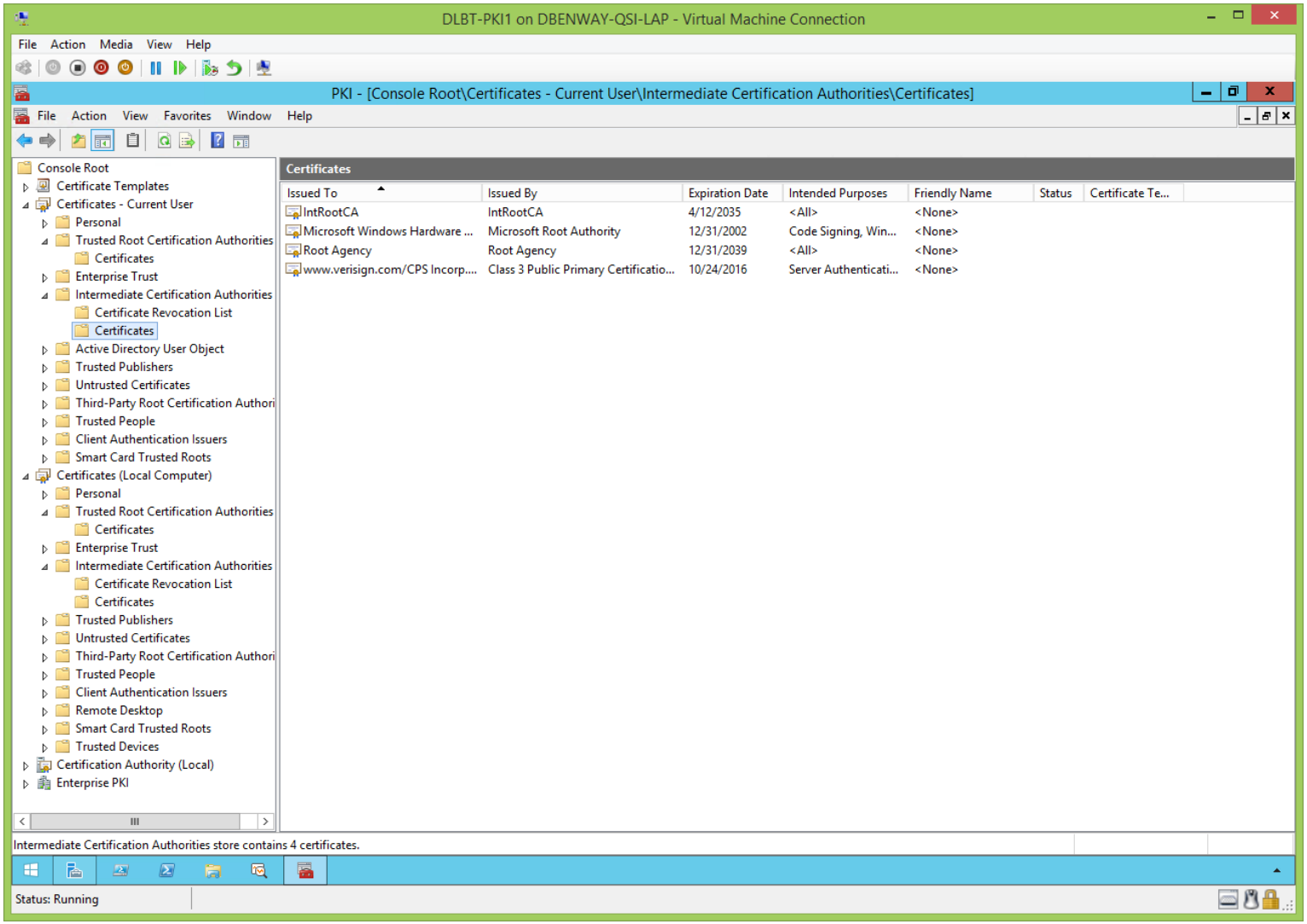


View root CA's local certificate store, cont'd.



Notice the dates on the root CA's certificate CRL have changed:

View root CA's local certificate store, cont'd.



View root CA's local certificate store, cont'd.

DLBT-PKI1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

PKI - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificate Templates
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authori
    - Trusted People
    - Client Authentication Issuers
    - Smart Card Trusted Roots
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authori
    - Trusted People
    - Client Authentication Issuers
    - Remote Desktop
    - Smart Card Trusted Roots
    - Trusted Devices
  - Certification Authority (Local)
  - Enterprise PKI

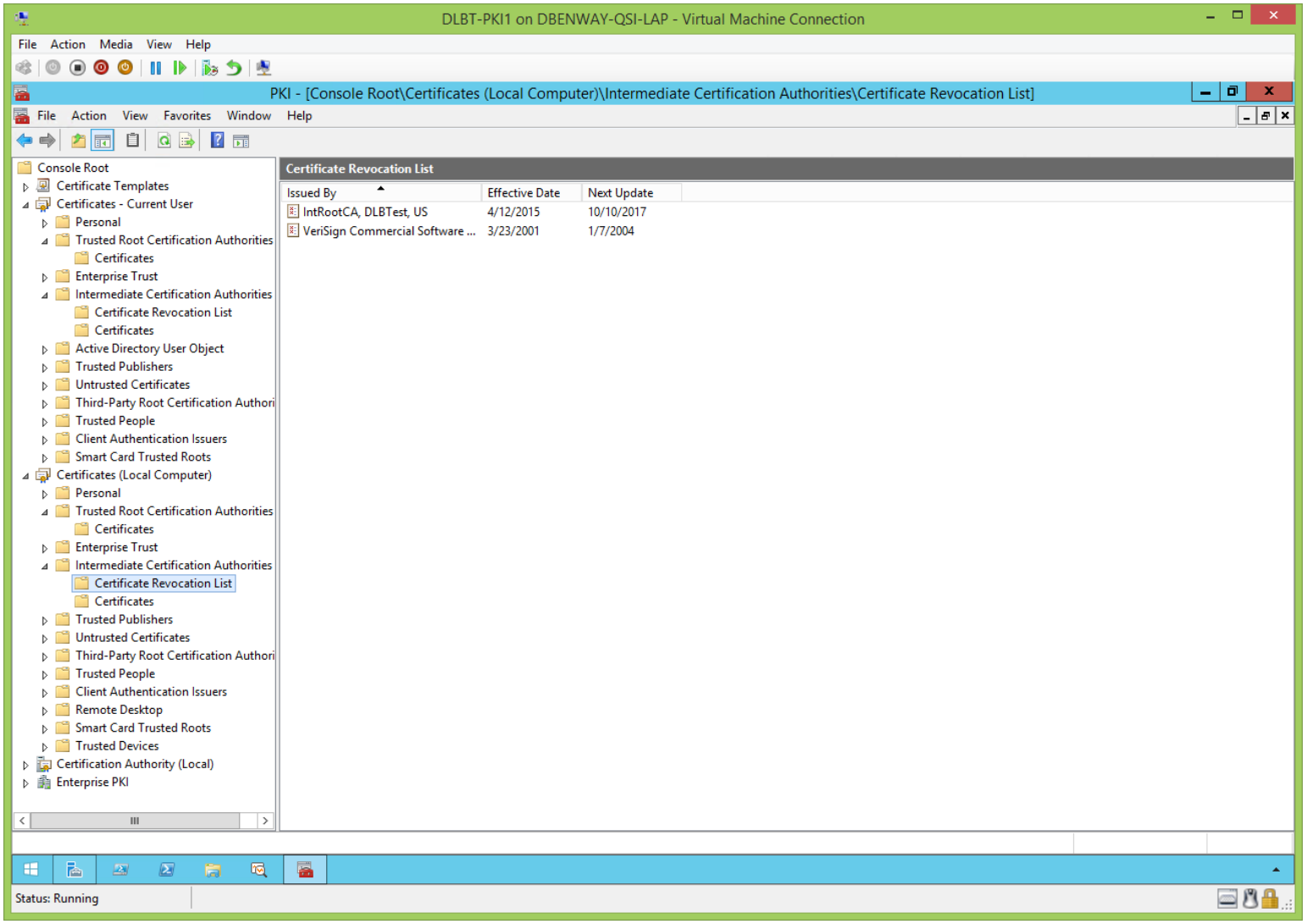
Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	Baltimore CyberTru...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
IntRootCA	IntRootCA	4/12/2035	<All>	<None>		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		

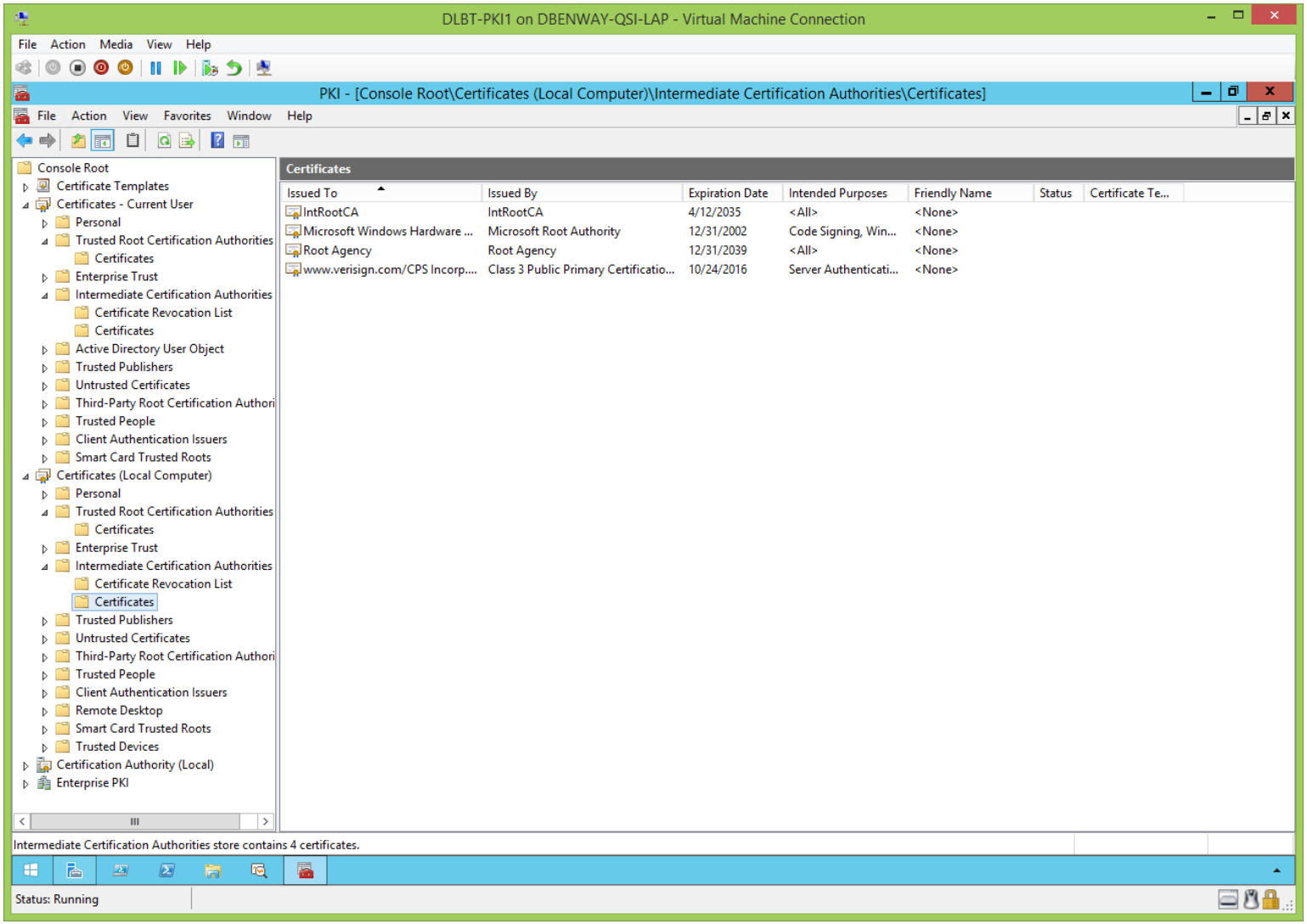
Trusted Root Certification Authorities store contains 12 certificates.

Status: Running

View root CA's local certificate store, cont'd.



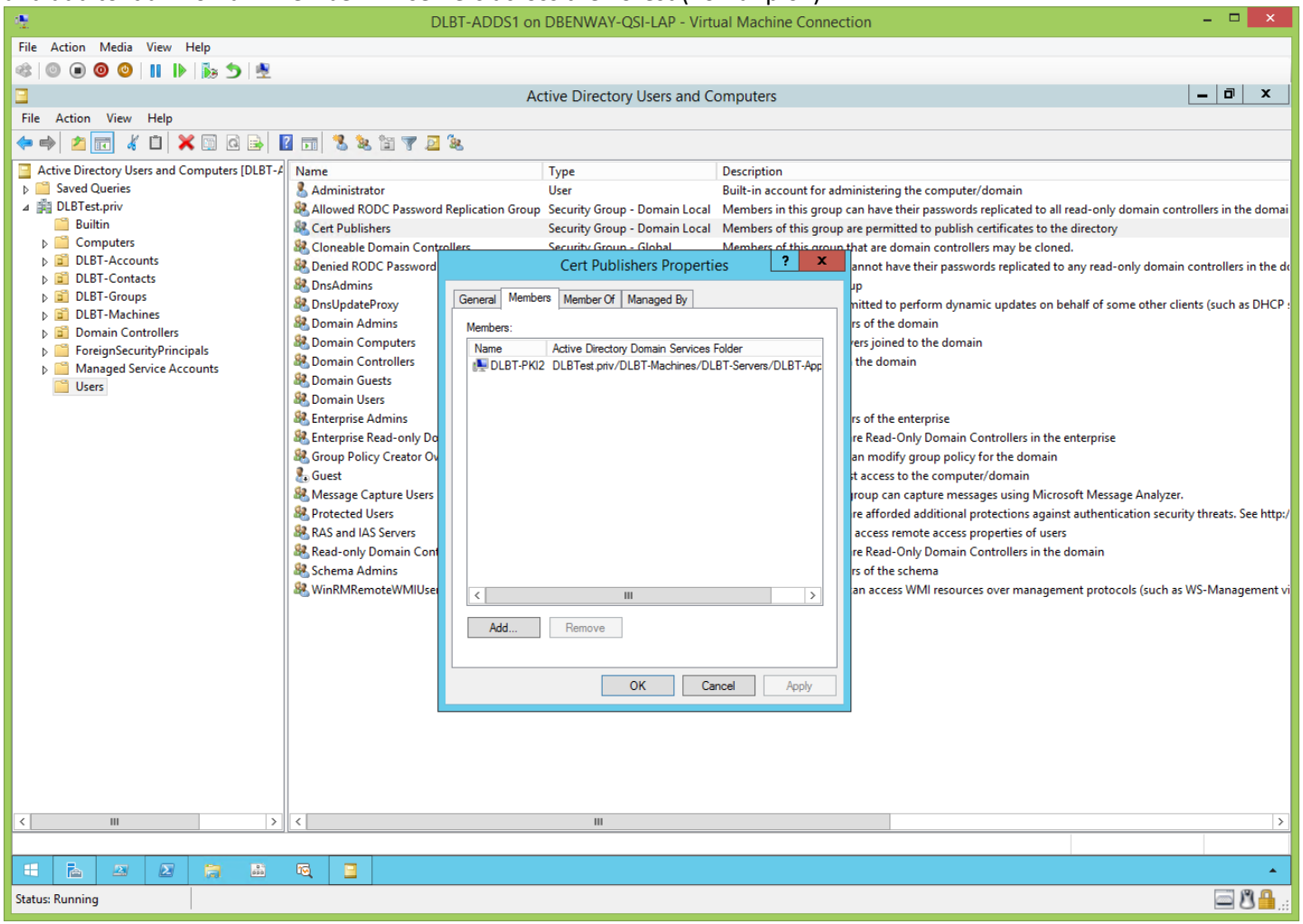
View root CA's local certificate store, cont'd.



Cert Publishers Group:

(jump to TOC)

Set the 'Cert Publishers' group in every Domain to be Domain Local (default in 2012 R2, but for other OSs a PowerShell script might be the only way to do this) and add to it all Domain-member PKI servers across the Forest (Komar p.67):



Note: members of the Domain Local 'Cert Publishers' security group have the right to publish certificates into the local Domain of the Active Directory.

OID:

(jump to TOC)

Get an OID which will be used to name each CP (Certificate Policy) on your policy CAs.

Obtaining an OID for a Certificate Issuing Policy (CAPolicy.inf)...
http://www.networkworld.com/article/2231566/microsoft-subnet/obtaining-an-oid-for-a-certificate-issuing-policy--capolicy-inf----.html

Method One:
If you already have a valid OID obtain a CPS arc from you OID overlord.

Method Two:
Don't have a valid OID? Go to the following Web site and after paying lots of money you too can become an evil OID overlord: http://web.ansi.org/other_services/registration_programs/reg_org.aspx?menuid=10 .

Method Three:
Go to the following site, and get OIDGen.vbs: http://gallery.technet.microsoft.com/ScriptCenter/en-us/56b78004-40d0-41cf-b95e-6e795b2e8a06. This script generates unique OIDs in the Microsoft number sequence (1.2.840.113556).

Method Four:
Cheat create your own. Bring up a backup of your Active Directory environment in a lab. Install certificate services as an Enterprise Root on a domain controller. At a command prompt on the domain controller type certtmpl.msc and press Enter. The Certificate Templates MMC will open. In the right pane select the Workstation Authentication template. Alternatively, you can select any other V2 template. From the Action menu select Properties. Click the Extensions tab. Select the Issuance Policies from the list box and click Edit. In the Edit Issuance Policies Extension dialog click Add. Click New... in the next dialog. A unique object identifier is generated and shown in the New Issuance Policy dialog. Select the complete OID and press + to copy the content into the clipboard. Copy the OID into a document for future reference.

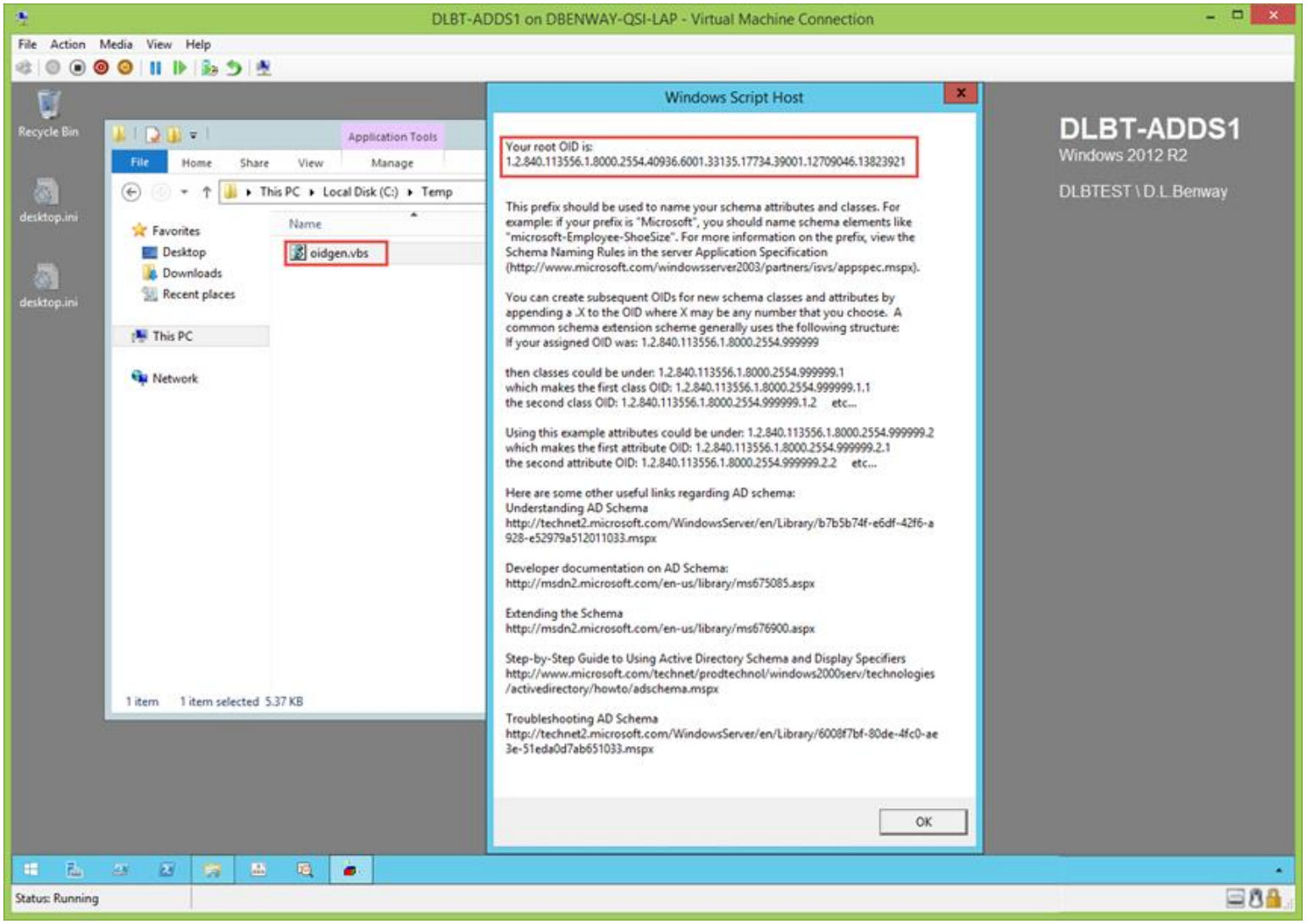
Again… this yet another procedure I wouldn't recommend for a "real" PKI deployment.

Obtaining an OID from MS (Method Three above)…
https://msdn.microsoft.com/en-us/library/ms677620(v=vs.85).aspx

> "Once you have a base OID, be careful when deciding how the OIDs should be divided into categories, because these OIDs are contained in the prefix table and are part of the DC replication data. It is recommended that no more than two OID categories be created." DLB: I think this means dividing up the OID, but not appending to it.
>
> "You can create subsequent OIDs for new schema classes and attributes by appending digits to the OID in the form of OID.X, where X may be any number that you choose." DLB: I think this means it's OK to append at will.

For an internal PKI you don't need a public OID, so use Microsoft's OIDGen.vbs to get your OID (for internal use only, not for external use):
OID for DLBTest: 1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921

Use OIDGen.vbs to generate an OID:



Devise a hierarchical plan for organizing your use of that OID, something like this:

1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921 is our OID

1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921**.001 is for AD schema extensions**
1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921**.002 is for PKI**
1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921**.002.001 is PKI CPs**
1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921**.002.001.001 is PKI CP 1**
1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921**.002.001.002 is PKI CP 2**
1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921**.003 is for SNMP**
1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921**.004-999 are TBD (room for growth)**

Now remember, "There is a practical limit to the number of certificate policies that can be included in a CA certificate. The Active Directory Domain Services (AD DS) schema allows only a maximum string length of 4,096 bytes for all CPS information, including OID, notification text, and URL. The total length of the certificate policy entries must be less than 4,096 bytes." (Komar p. 104)

In ASCII every character takes up one byte (8 bits), but in UniCode every character takes up two bytes (16 bits).

Sub/Policy/Issuing CA:

(jump to TOC)

This page is just a TOC placeholder.

Sub/Policy/Issuing CA's CAPolicy.inf (Before CertUtil.exe):

(jump to TOC)

WARNING: This CAPolicy.inf file has a lot of important comments that need to be read and understood, or problems will arise.
Note: Because the CAPolicy.inf and Certutil.exe files in this document have been updated since initial publication, the values in this document's screenshots (such as registry settings, publication intervals, etc.) might not always reflect the values from these files.

To build the sub/policy/issuing CA, first write (in %SystemRoot%) the CAPolicy.inf file:

```
;-----------------------------------------------------------------------------------------------------------------------------------------------------
; CAPolicy.inf Sub/Policy/Issuing
;
; CAPolicy.inf is used during ADCS installation of the local CA, and renewal of the local CA's certificate.
; Save it in %systemRoot% in ANSI format.
; Remember to never install a CA on a DC (it's a violation of best practice).
; Be sure to follow the PathLength procedure at the end of this CAPolicy.inf file.
;-----------------------------------------------------------------------------------------------------------------------------------------------------

;#####################################################################################################################################################
[Version]
Signature="$Windows NT$"

;#####################################################################################################################################################
[PolicyStatementExtension]
;-----------------------------------------------------------------------------------------------------------------------------------------------------
; See RFC 3647 for more info: https://www.ietf.org/rfc/rfc3647.txt
;-----------------------------------------------------------------------------------------------------------------------------------------------------
Policies=DLBTestCP

;#####################################################################################################################################################
[DLBTestCP]
;-----------------------------------------------------------------------------------------------------------------------------------------------------
; See RFC 3647 for more info: https://www.ietf.org/rfc/rfc3647.txt
;-----------------------------------------------------------------------------------------------------------------------------------------------------
OID=1.2.840.113556.1.8000.2554.40936.6001.33135.17734.39001.12709046.13823921.002.001.001
NOTICE=Notice: DLBTest CP (Certificate Policy)
URL=http://PKI.DLBTest.priv/CP/DLBTestCP.txt

;#####################################################################################################################################################
[CertSrv_server]
;-----------------------------------------------------------------------------------------------------------------------------------------------------
; This sub/policy/issuing CA's certificate will be signed by the root CA.
; This sub/policy/issuing CA's certificate has a key length, and a certificate validity period which is specified during its local ADCS installation GUI
; wizard.
; The key length and validity period of the certificates this sub/policy/issuing CA issues is specified in the enterprise templates (standalone CAs
; configure validity periods for the certificates they issue in their registry, enterprise CAs do it in the enterprise templates (and if not there then it
; defaults to their registry)).
;-----------------------------------------------------------------------------------------------------------------------------------------------------
; These renewal settings affect renewal of this sub/policy/issuing CA's certificate (because there is no enterprise template which defines them, and
;       because the local ADCS installation GUI would have already been run at the time of renewal).
; During renewal these settings will default to match the existing certificate. They have been explicitly set here for completeness and clarity.
; Key length 2048 is chosen for compatibility.
; The lowest certificates should have up to 5 years, so sub/policy/issuing CA's certificate is 10, so root CA's certificate is 20.
;-----------------------------------------------------------------------------------------------------------------------------------------------------
```

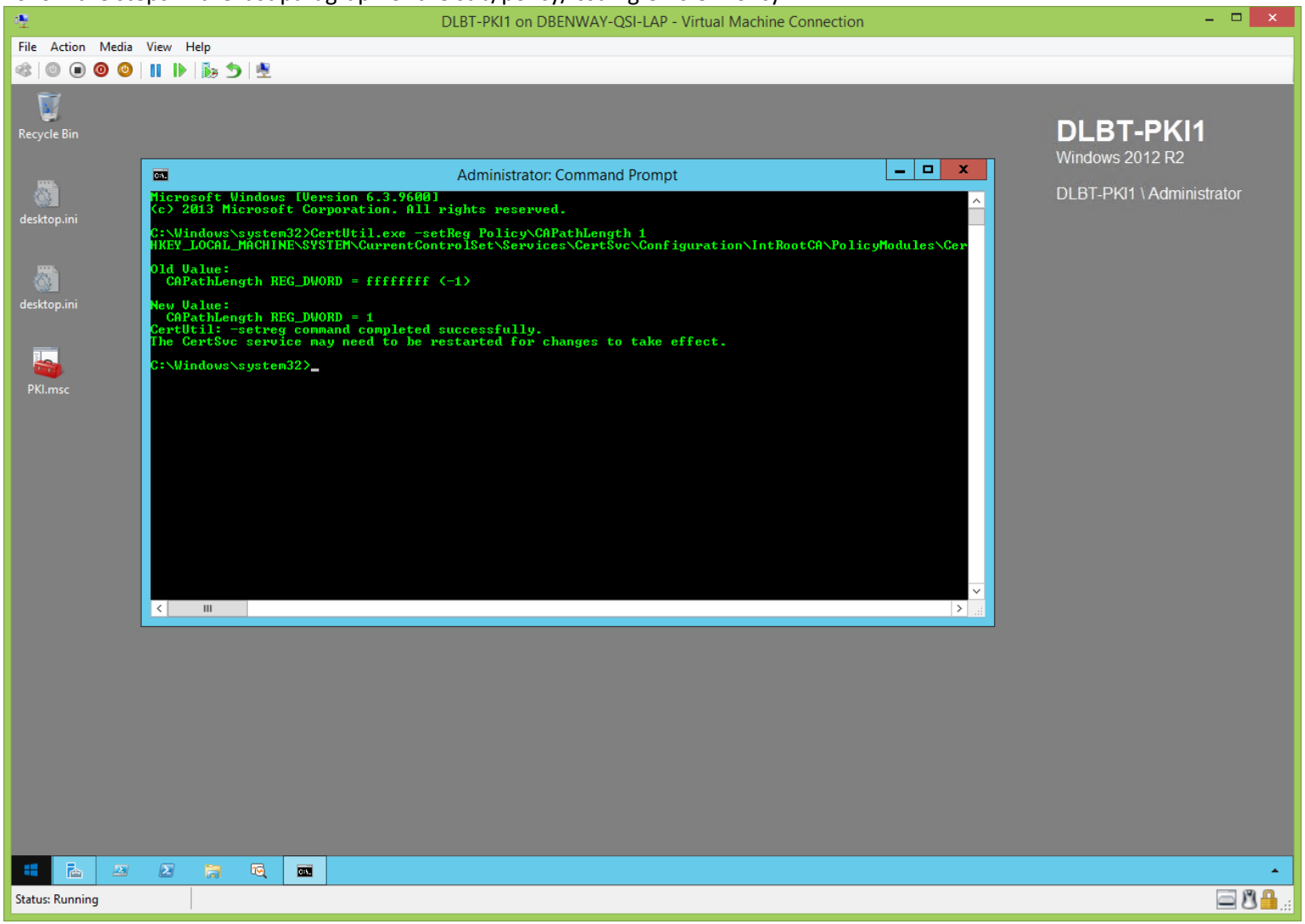
```
RenewalKeyLength=2048
RenewalValidityPeriodUnits=10
RenewalValidityPeriod=years

;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; We want to support Windows OSs earlier than Vista, as well as Apple, Cisco, Java, etc., so disable alternate signatures for the certificates this
; sub/policy/issuing CA issues.
; Note: 'Discrete' has been deprecated and replaced by 'Alternate'.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
AlternateSignatureAlgorithm=0

;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; LoadDefaultTemplates=0 means do NOT issue the default certificate templates onto this sub/policy/issuing CA from the AD.
; LoadDefaultTemplates=1 means issue the default certificate templates onto this sub/policy/issuing CA from the AD.
; WARNING: Please research and carefully consider whether or not you want to use these default certificate templates.
; Most PKI experts agree that it's best practice to NOT load default templates.
; If you don't load them, this CA will only issue certificates based on templates you specifically issue from AD onto this CA (giving you the opportunity
; to customize the templates before issuing them onto this CA). This is good for complex PKIs that are actively managed by experienced admins.
; If you do load them, this CA will issue certificates based on the default templates. This might be OK for a lab or for simpler PKIs that are more casually
; managed by less experienced admins. Some certificates will be automatically issued (such as for Domain Controllers) because the default templates were
; loaded.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
LoadDefaultTemplates=1

;###########################################################################################################################################################
; [CRLDistributionPoint]
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; This section is not needed by a sub CA because it gets the CDP settings in its CA certificate from its superior's CDP extensions.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------

;###########################################################################################################################################################
; [AuthorityInformationAccess]
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; This section is not needed by a sub CA because it gets the AIA settings in its CA certificate from its superior's AIA extensions.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------

;###########################################################################################################################################################
[BasicConstraintsExtension]
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; The subject type in this root CA's certificate is 'CA'.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
Subject Type=CA

;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; PathLength should be set on the policy CA, not the root CA, to provide the greatest future flexibility for change.
; PathLength of zero means this CA is an end node in the CA hierarchy.
; In 2012 R2, 2016, and 2019 it seems that setting the sub/policy/issuing CA's PathLength in the CAPolicy.inf just doesn't work so:
;       1. completely build and configure the root CA
;       2. on the root CA run "CertUtil.exe -setReg Policy\CAPathLength 1" from an administrative command prompt
;       3. restart ADCS on the root CA
;       4. completely build and configure the sub/policy/issuing CA
;       5. on the root CA run "CertUtil.exe -setReg Policy\CAPathLength 0xffffffff" from an administrative command prompt (which sets
;                the root CA's PathLength back to none)
;       6. restart ADCS on the root CA
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
PathLength=0

;-----------------------------------------------------------------------------------------------------------------------------------------------------------
; This section may not be skipped.
;-----------------------------------------------------------------------------------------------------------------------------------------------------------
```

```
Critical=true
```

Sub/Policy/Issuing CA's Path Length Preparation (Before CertUtil.exe):

(jump to TOC)

Follow the steps in the last paragraph of the sub/policy/issuing CA's CAPolicy.inf:



Verify the Registry setting change on the root CA, then restart the root CA's ADCS:

DLBT-PKI1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

Registry Editor

File Edit View Favorites Help

bxfcoe
bxois
cdfs
cdrom
CertPropSvc
CertSvc
Configuration
IntRootCA
CSP
EncryptionCSP
ExitModules
PolicyModules
CertificateAuthority_MicrosoftD
Performance
Security
cht4vbd
CLFS
clr_optimization_v4.0.30319_32
clr_optimization_v4.0.30319_64
CmBatt
CNG
CngHwAssist
CompositeBus
COMSysApp
condrv
crypt32
CryptSvc
DCLocator
DcomLaunch
defragsvc
DeviceAssociationService
DeviceInstall
Dfsc
Dhcp
disk
dmvsc
Dnscache
dot3svc

Name	Type	Data
(Default)	REG_SZ	(value not set)
CAPathLength	REG_DWORD	0x00000001 (1)
DefaultSMIME	REG_MULTI_SZ	1.2.840.113549.3.2,128 1.2.840.113549.3.4,128 1.3.14.3.2.7 1.2.840.113549.3.7
DisableExtensionList	REG_MULTI_SZ	
EditFlags	REG_DWORD	0x000083ee (33774)
EnableEnrolleeRequestExtensionList	REG_MULTI_SZ	1.3.6.1.4.1.311.10.9.1 1.3.6.1.4.1.311.20.2 1.3.6.1.4.1.311.21.7 1.3.6.1.4.1.311.21.10 1.3.6.1.4.1.311.21.11 1.3.6.1.4.1.311.21.12 2
EnableRequestExtensionList	REG_MULTI_SZ	1.2.840.113549.1.9.15 1.3.6.1.4.1.311.21.1 1.3.6.1.4.1.311.21.2 2.5.29.15
RequestDisposition	REG_DWORD	0x00000101 (257)
RevocationType	REG_DWORD	0x00000100 (256)
RevocationURL	REG_SZ	https://%1/CertEnroll/nsrev_%3.asp
SubjectAltName	REG_SZ	DISABLED: Set to EMail to set SubjectAltName extension to the email address
SubjectAltName2	REG_SZ	DISABLED: Set to EMail to set SubjectAltName2 extension to the email address

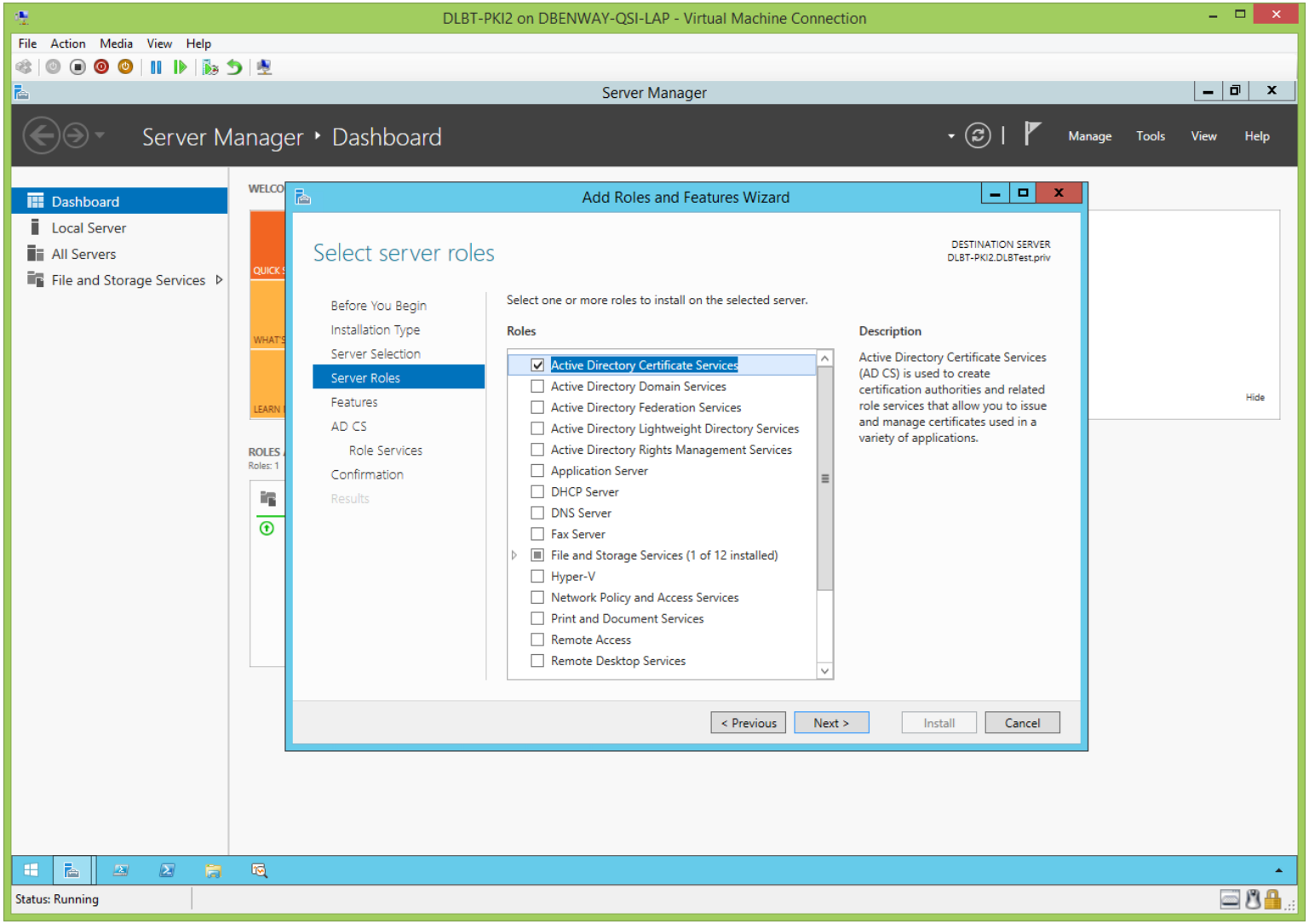
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\IntRootCA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy

Status: Running

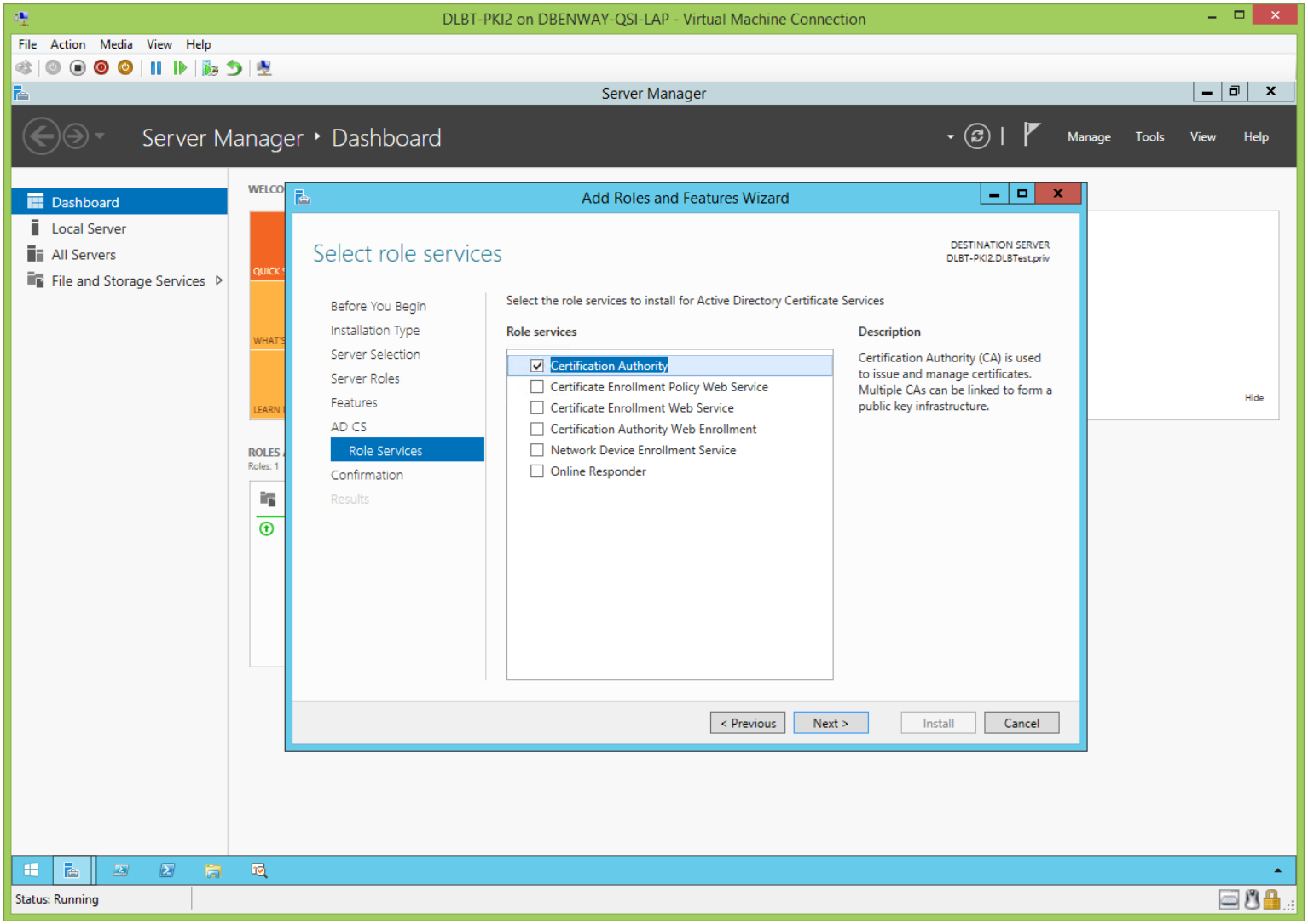
Sub/Policy/Issuing CA's ADCS Installation Wizard (Before CertUtil.exe):

(jump to TOC)

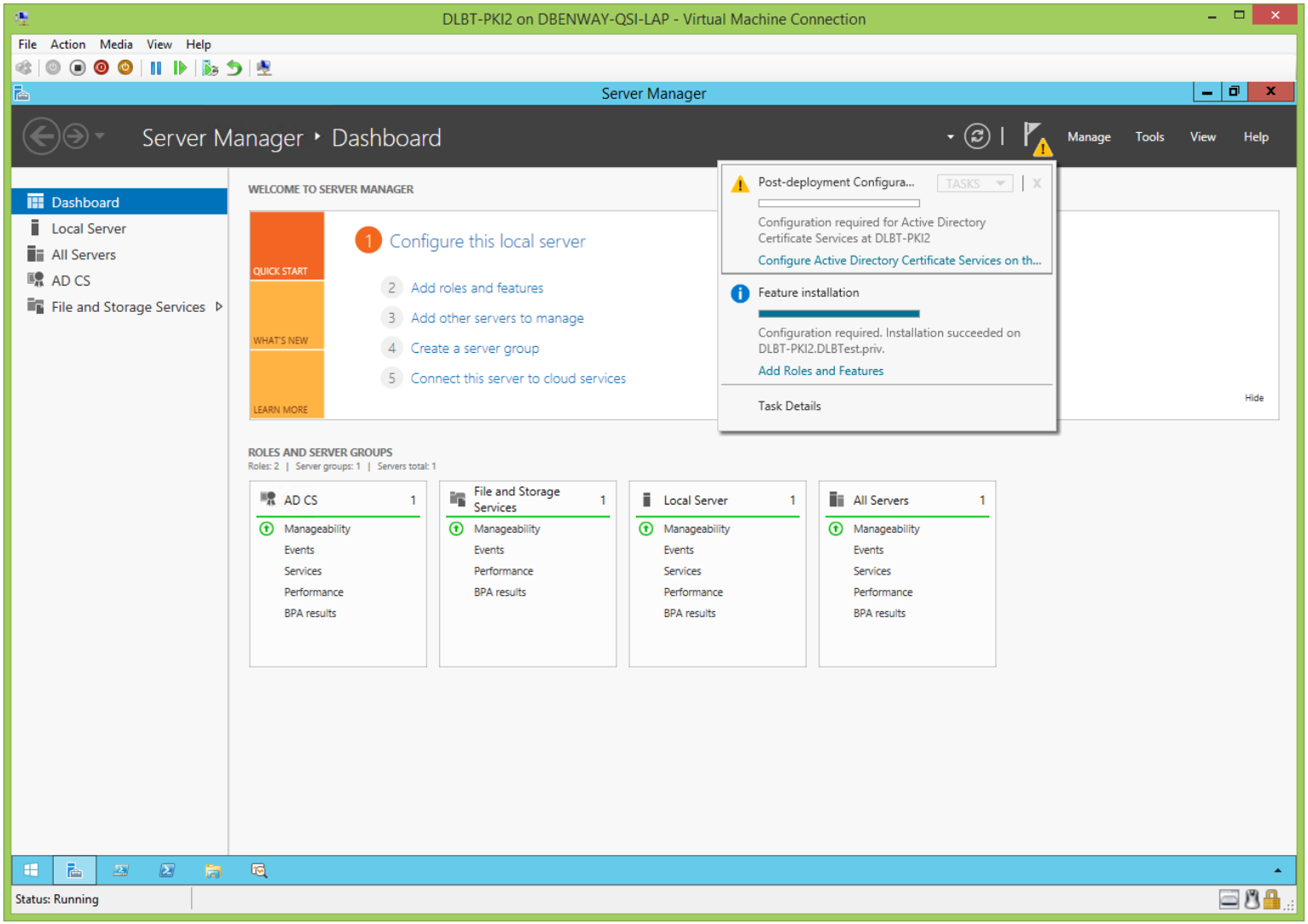
Install ADCS onto the sub/policy/issuing CA:



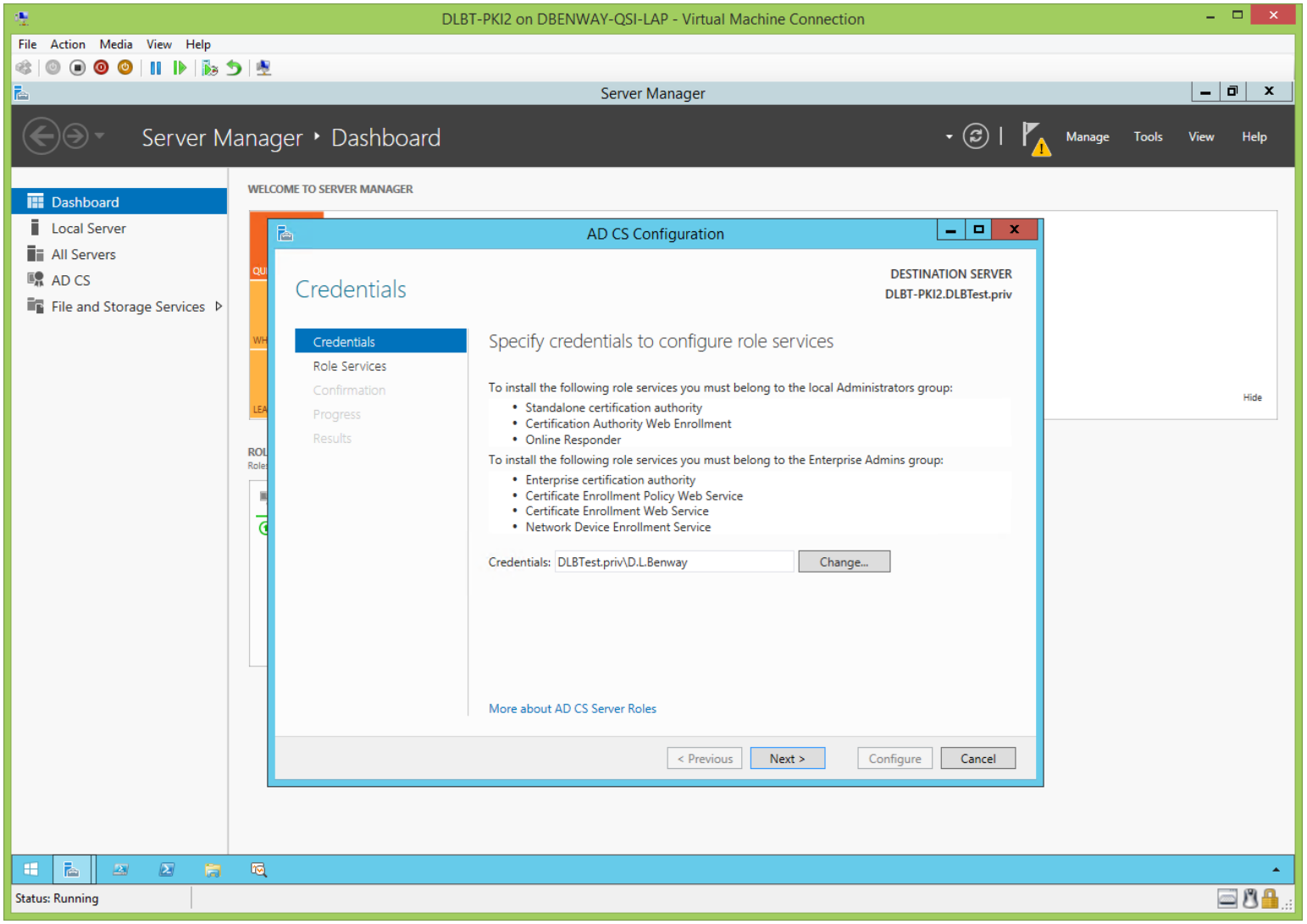
Certifiaction Authority is the only needed role:



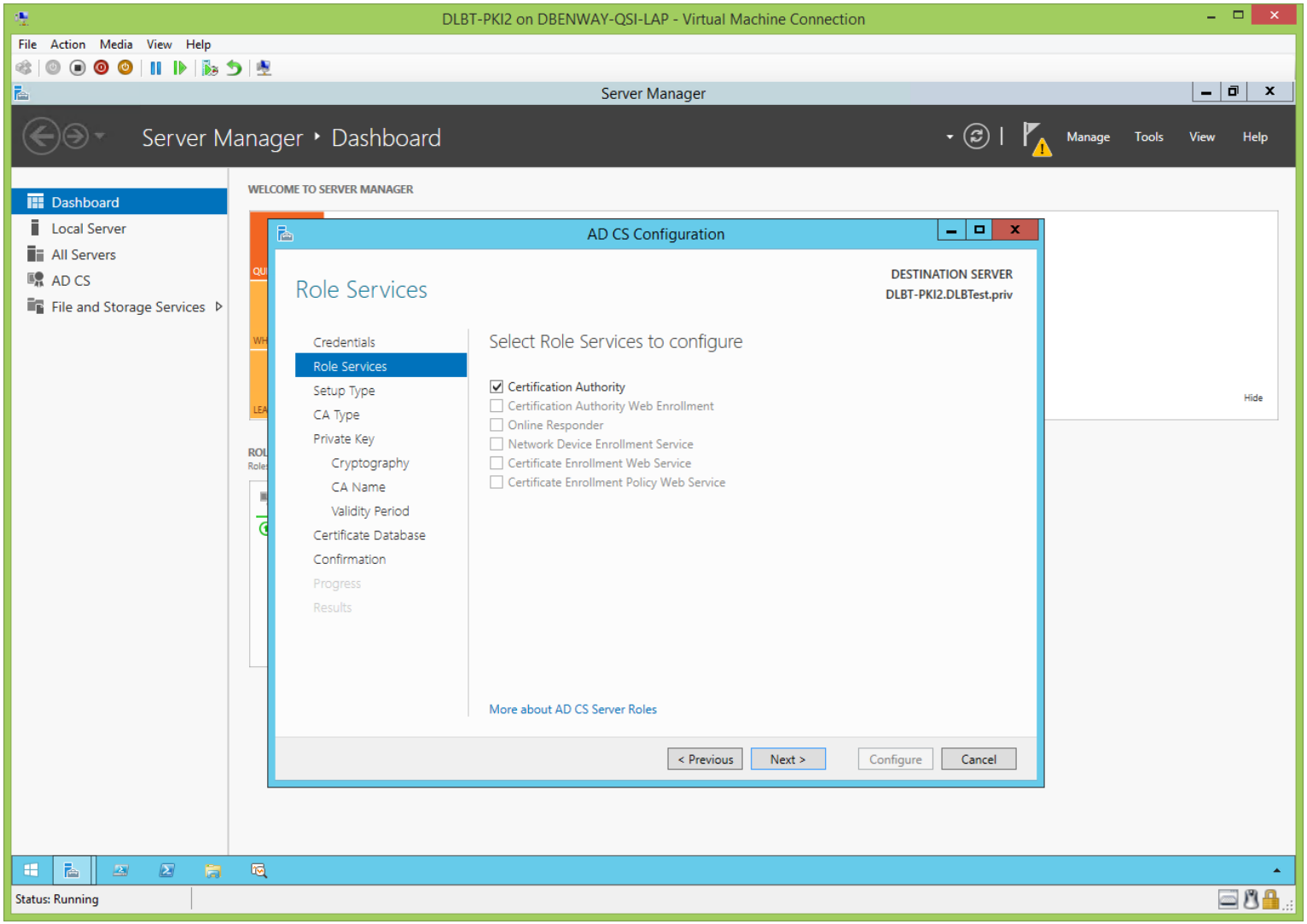
After installation of ADCS, we need to configure the sub/policy/issuing CA:



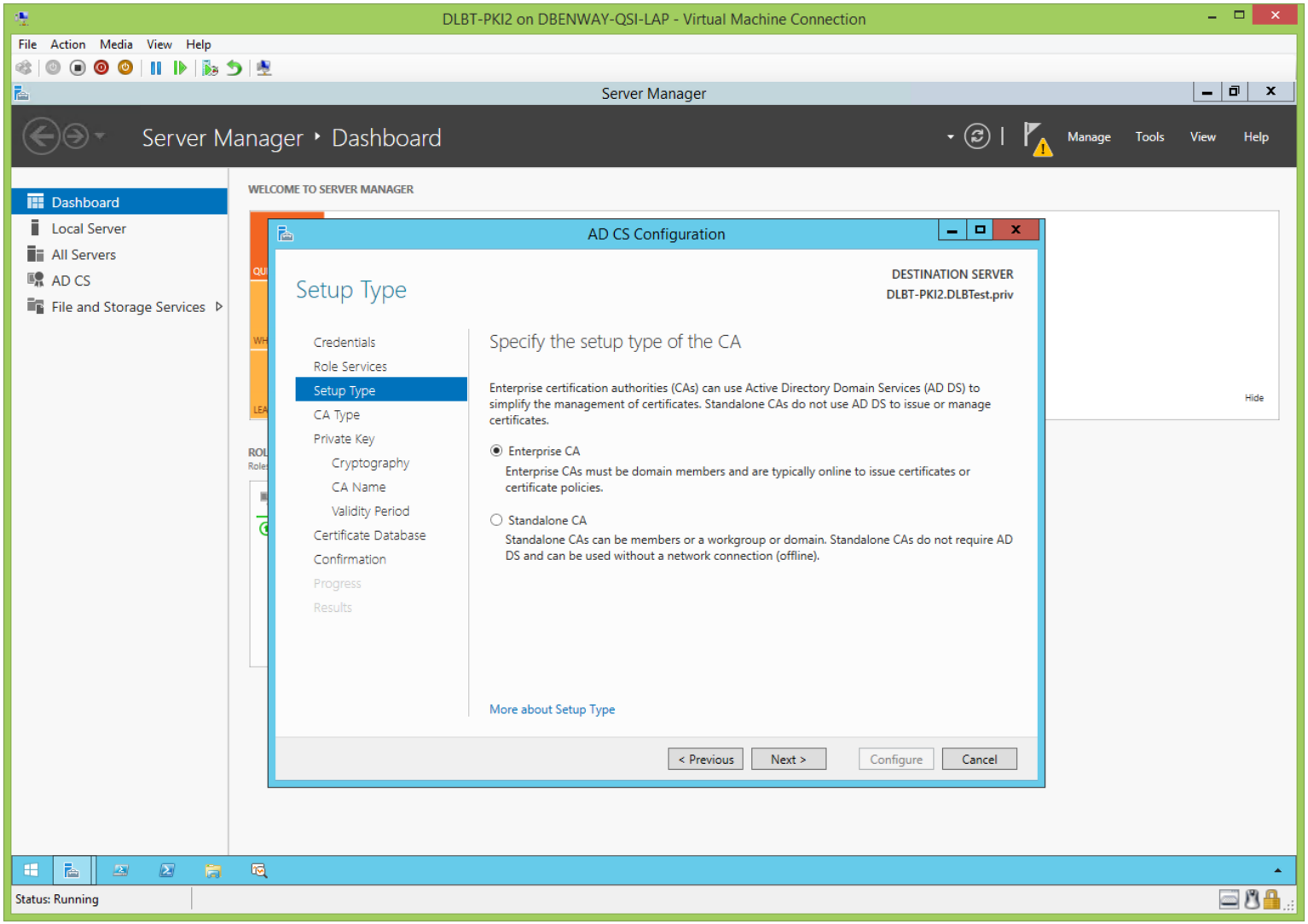
Use an account with sufficient permissions (an Enterprise Admin who is also a member of the sub/policy/issuing CA's local Administrators group):



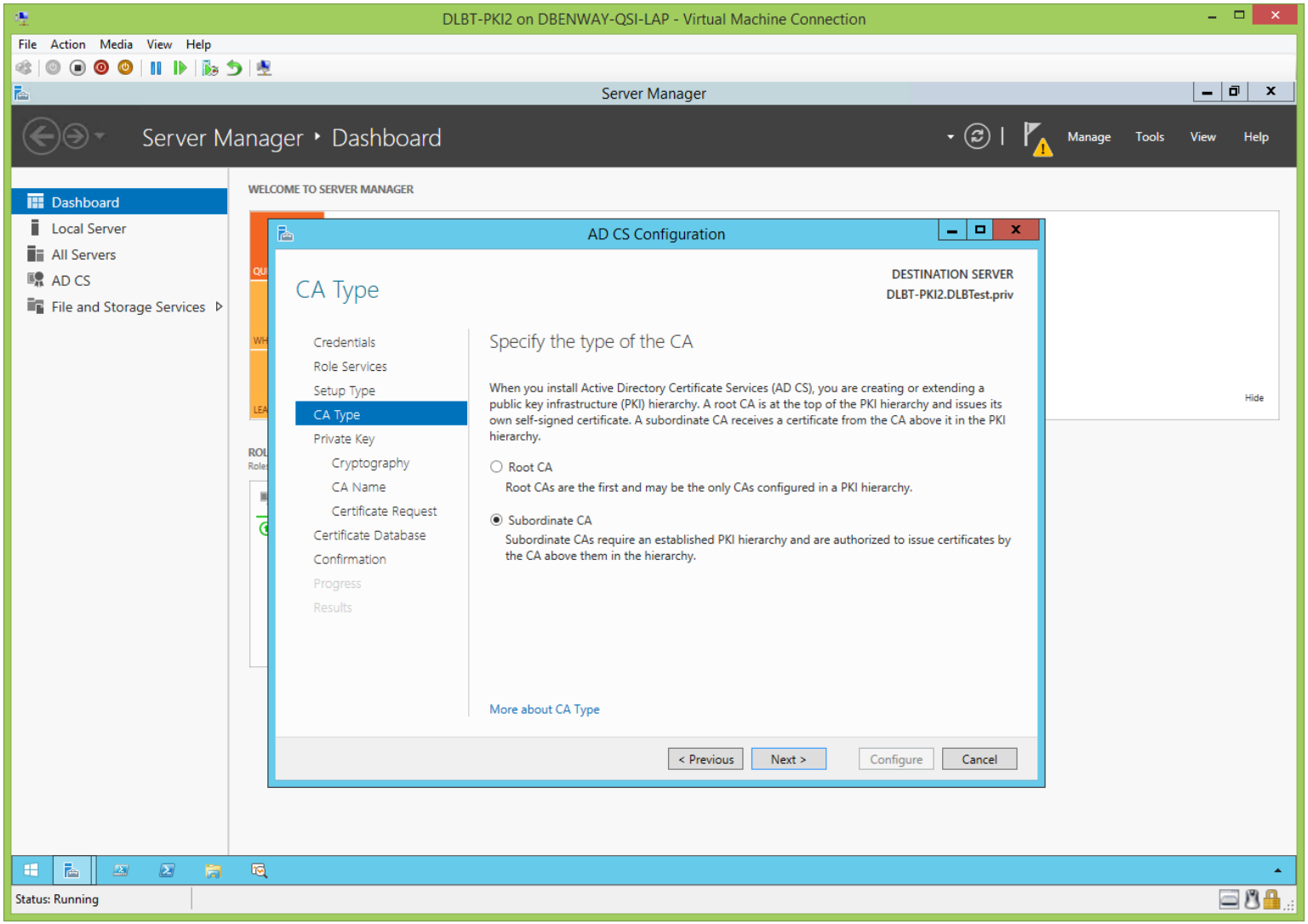
Certification Authority is the only role to configure:



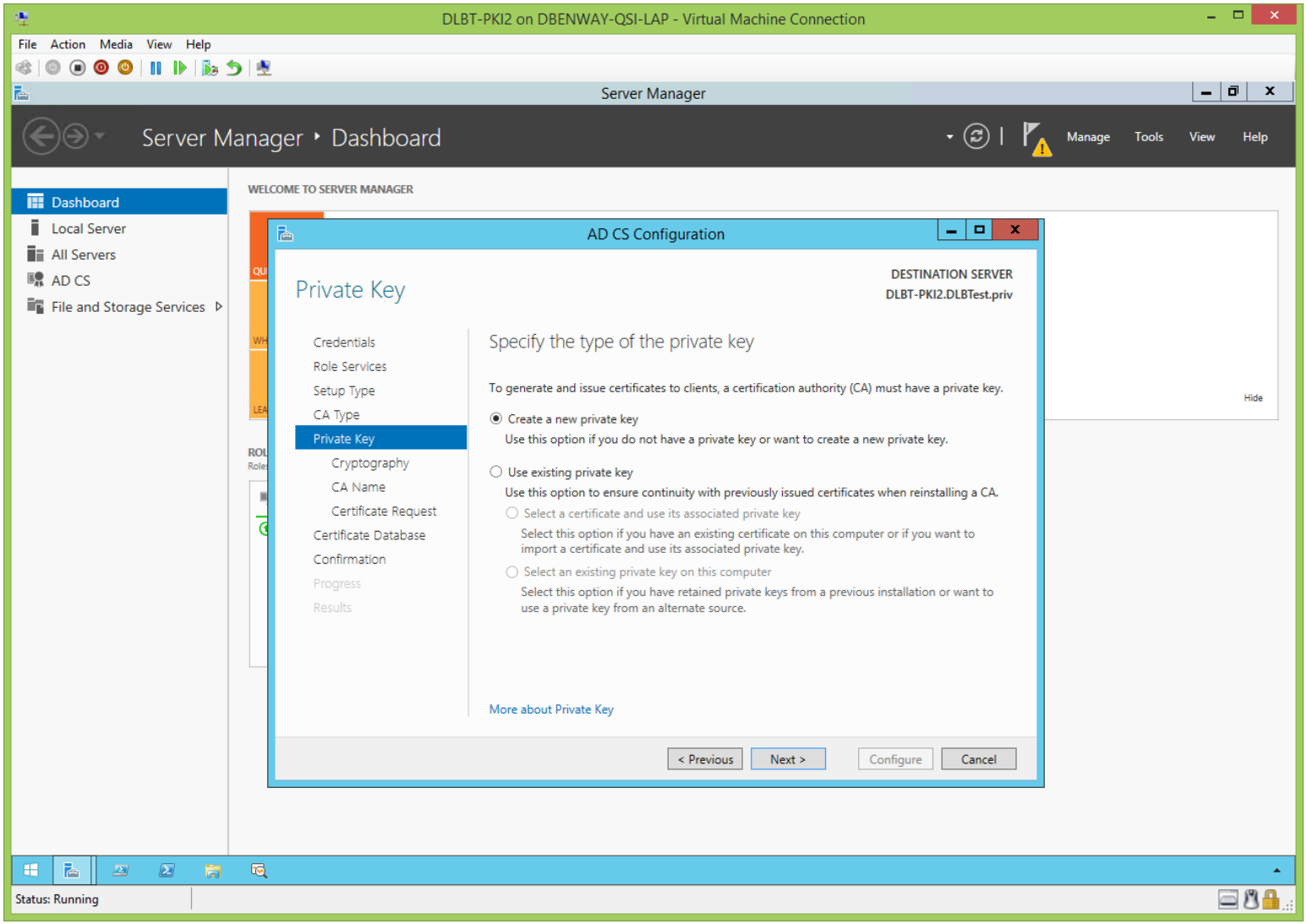
This sub/policy/issuing CA will be an Enterprise sub/policy/issuing CA (it will be a Domain member):



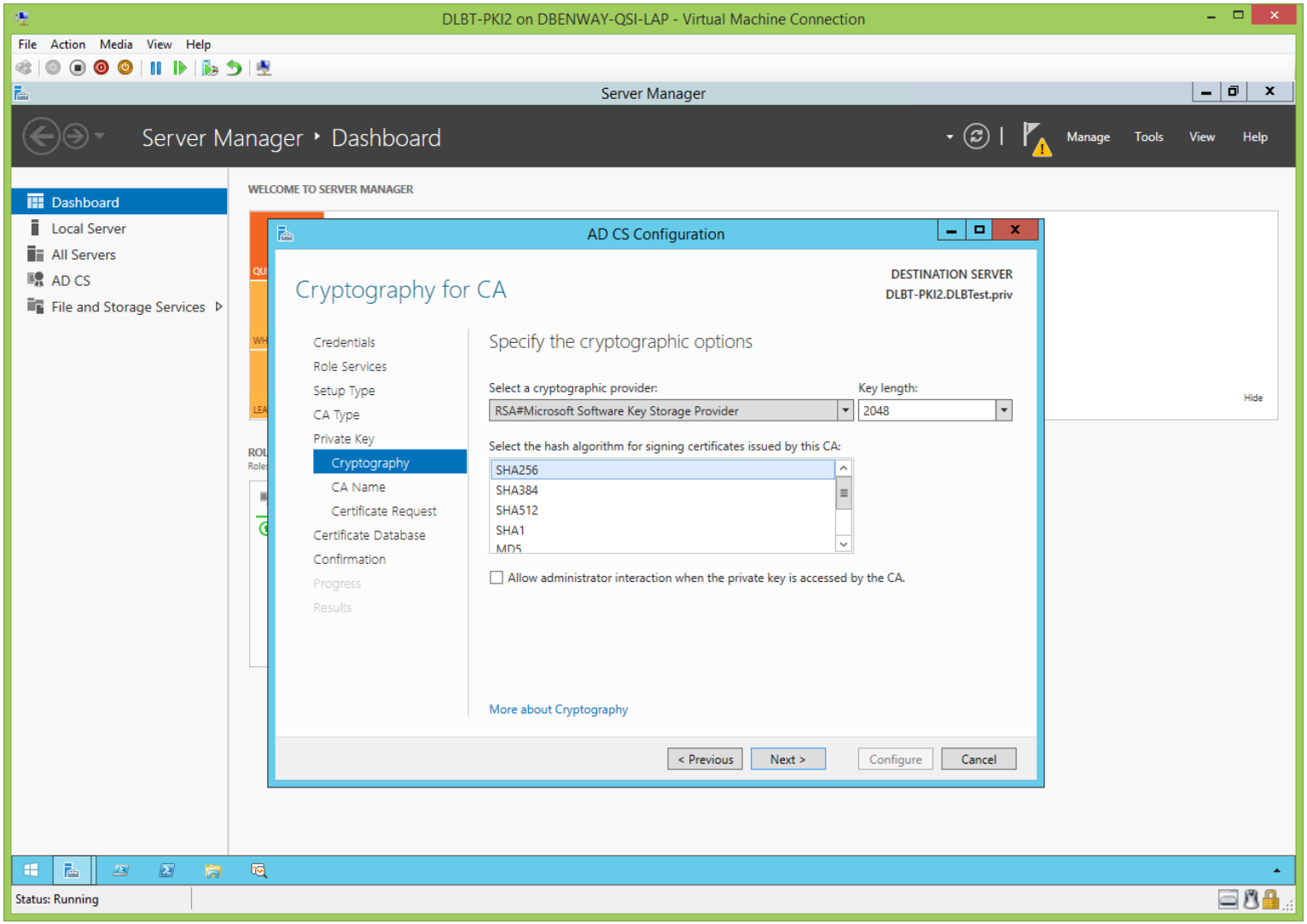
This sub/policy/issuing CA will be subordinate to the root CA:



This is a new CA, so we'll create a new private key for this sub/policy/issuing CA:

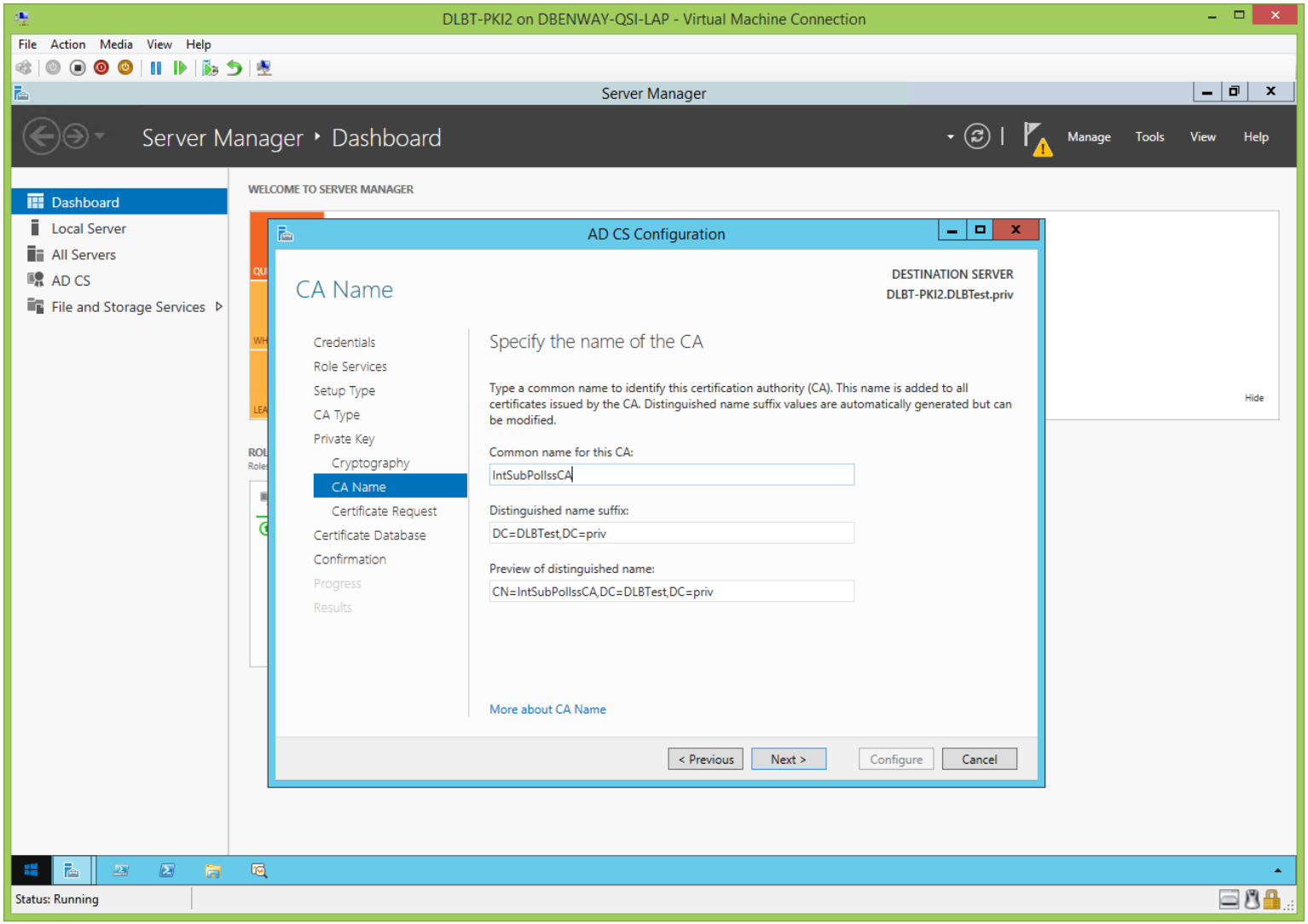


- Microsoft's software Key Storage Provider (MS KSP) will be the Cryptographic Storage Provider (CSP) used by this sub/policy/issuing CA.
- Key length 2048 is just for this sub/policy/issuing CA's certificate. 2048 was chosen because it's highly compatible.
- SHA256 is the hash algorithm used by this sub/policy/issuing CA (SHA1 is no longer secure, so don't use it).

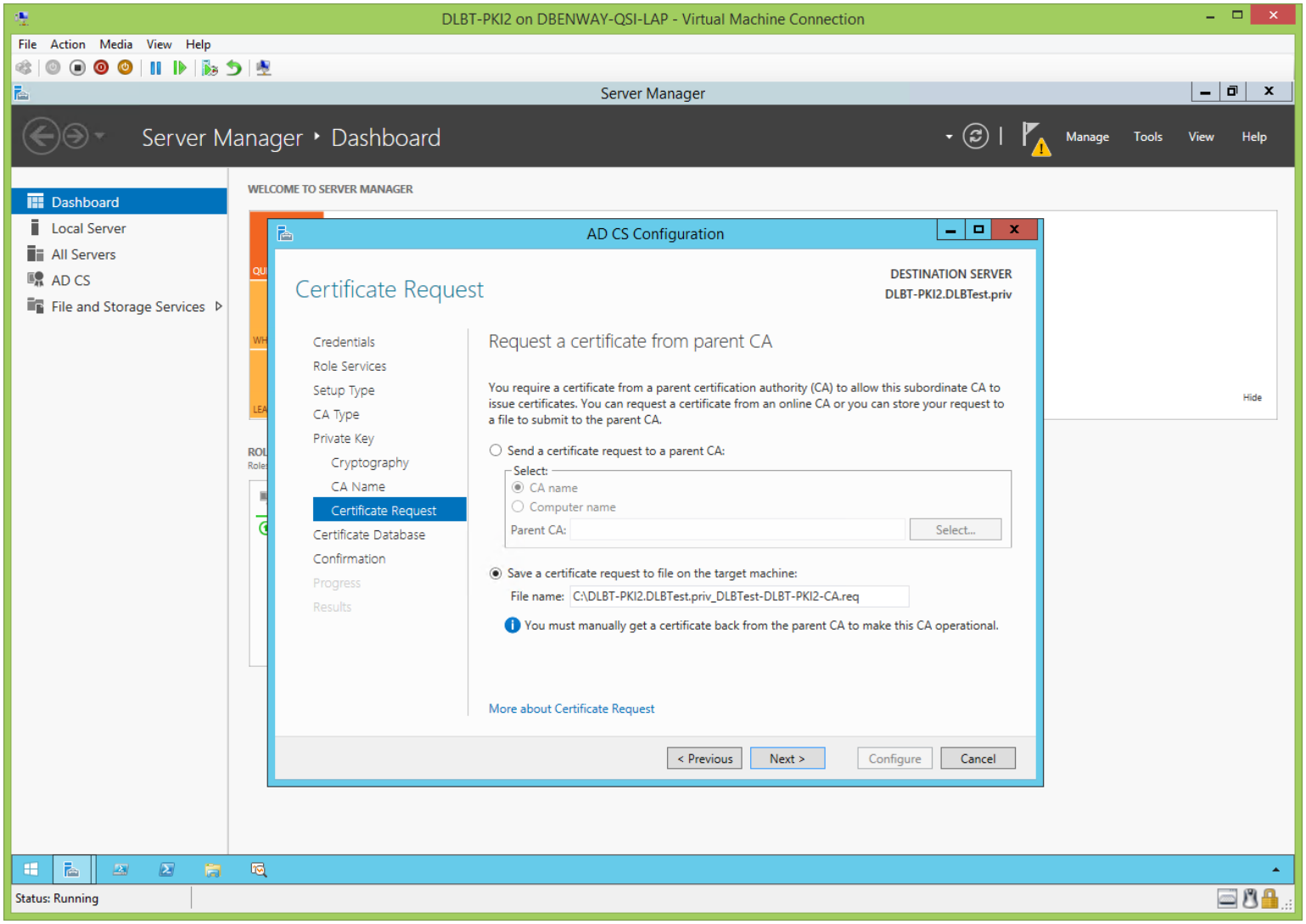


Give this sub/policy/issuing CA a meaningful name (not identical to its hostname) like IntPolIssCA. I like to keep the name to 15 or fewer characters in case there's a NetBIOS compatibility issue.

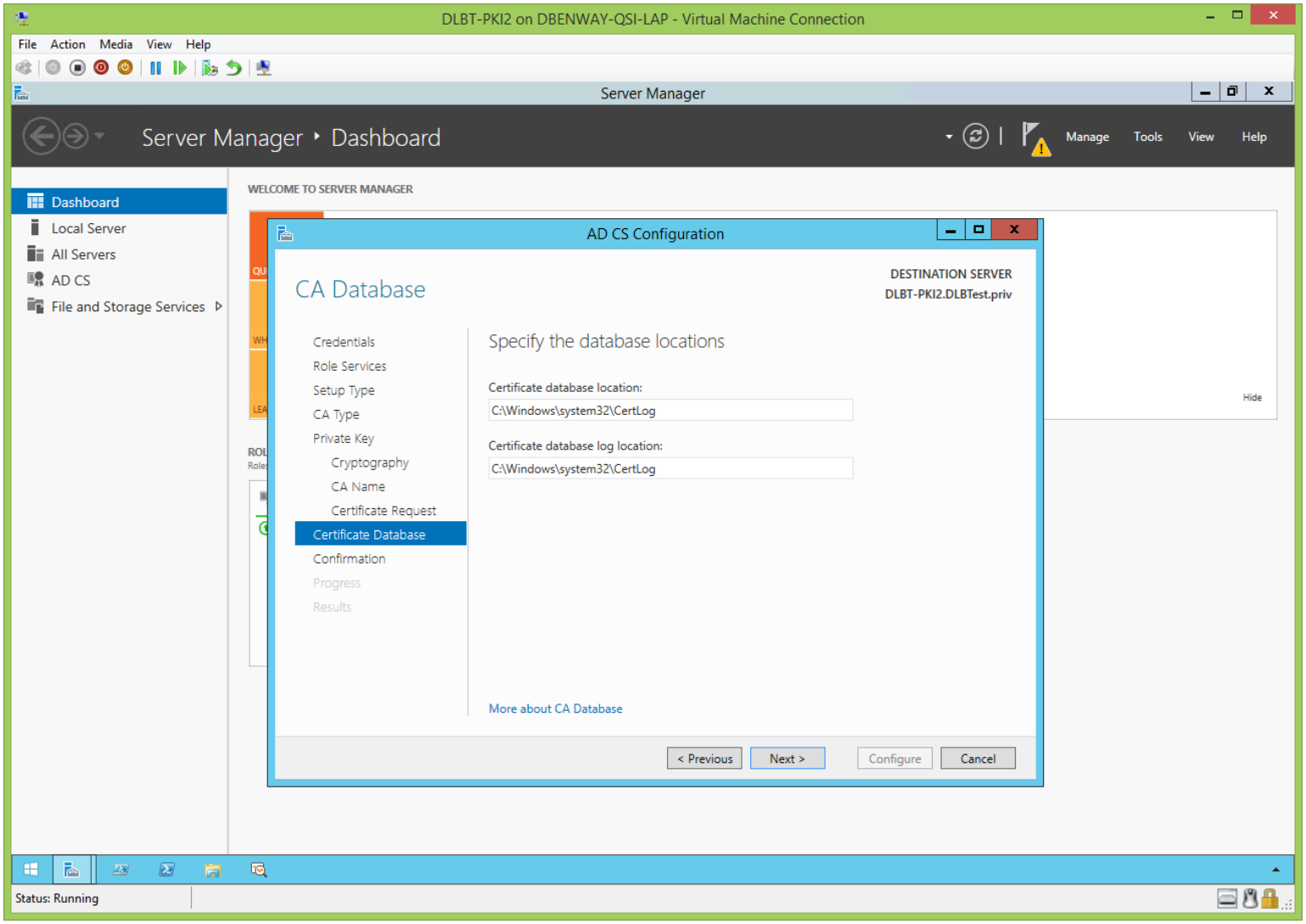
The distinguished name suffix is usually the system's AD distinguished name minus its hostname:



Because the root CA is offline, we'll have to save this sub/policy/issuing CA's certificate request to a file:



Set the desired location for the local ADCS database and logs:



Review the configuration:

DLBT-PKI2 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

Server Manager

Server Manager ‣ Dashboard

Manage Tools View Help

Dashboard
Local Server
All Servers
AD CS
File and Storage Services

WELCOME TO SERVER MANAGER

AD CS Configuration

Confirmation

DESTINATION SERVER
DLBT-PKI2.DLBTest.priv

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

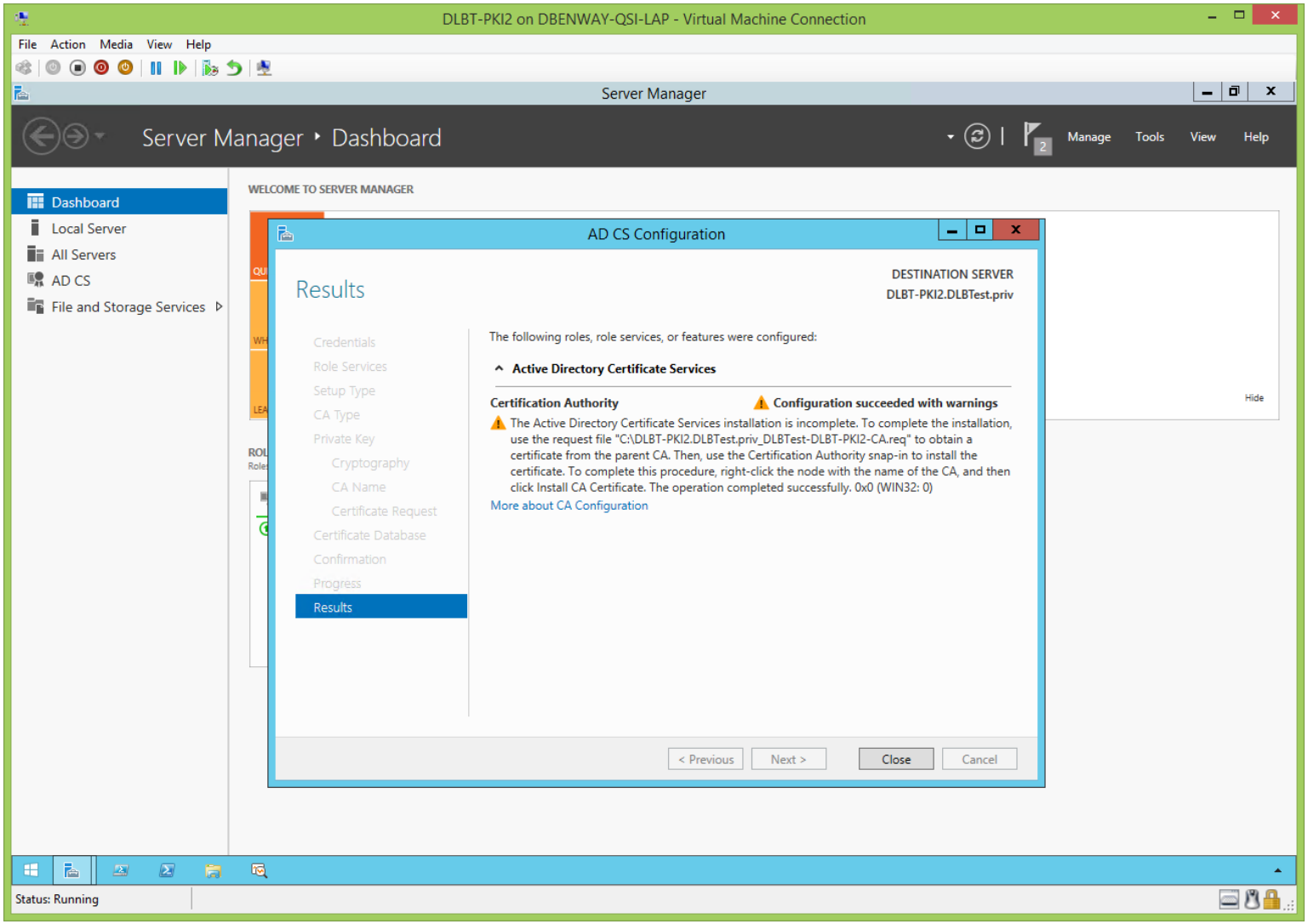
CA Type:	Enterprise Subordinate
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	Determined by the parent CA
Distinguished Name:	CN=IntSubPolIssCA,DC=DLBTest,DC=priv
Offline Request File Location:	C:\DLBT-PKI2.DLBTest.priv_DLBTest-DLBT-PKI2-CA.req
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

< Previous Next > Configure Cancel

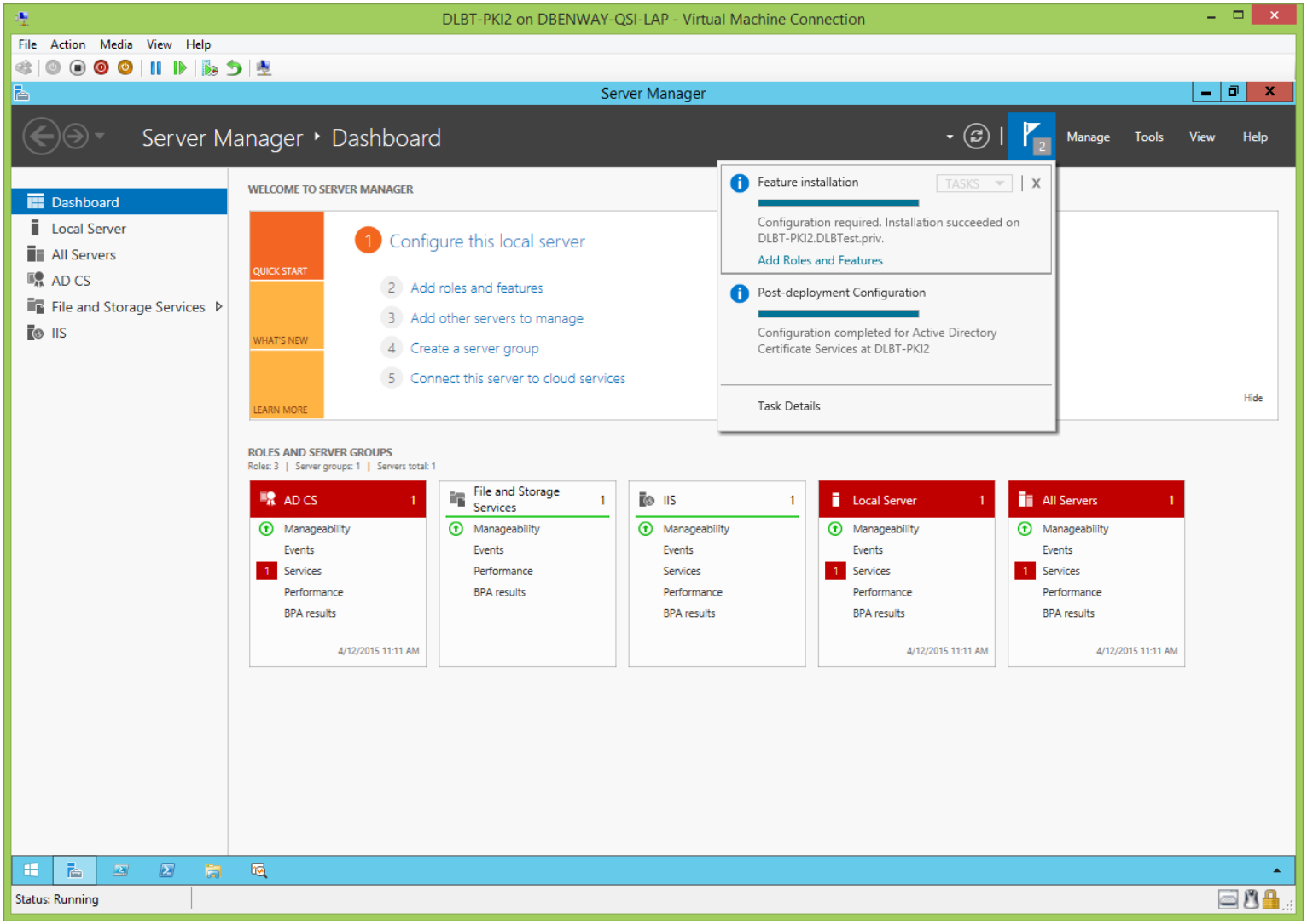
Hide

Status: Running

Configuration will be complete once this sub/policy/issuing CA requests and then installs its CA certificate from the root CA:



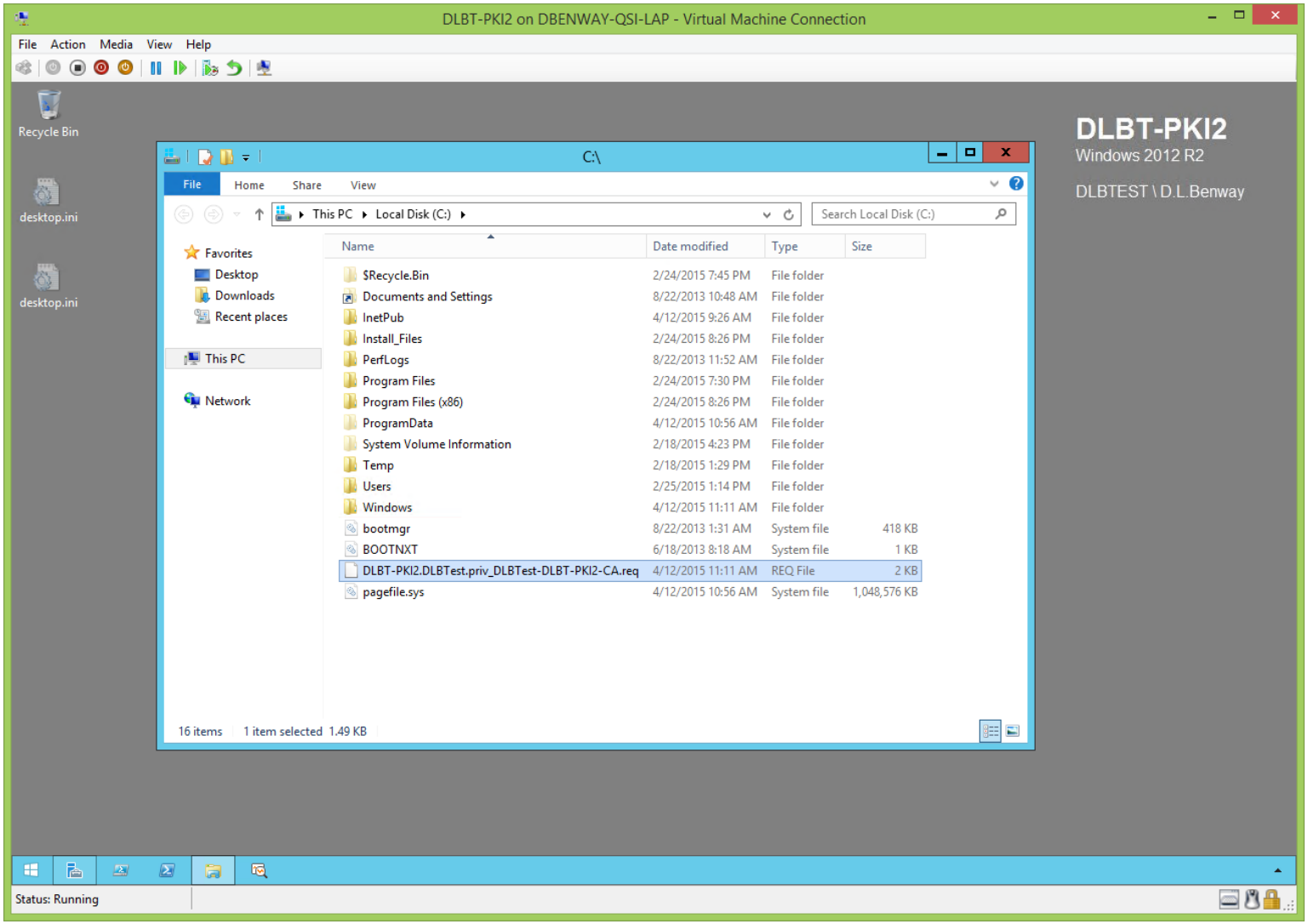
ADCS installation is complete, but this sub/policy/issuing CA still needs to request and then install its CA certificate from the root CA:



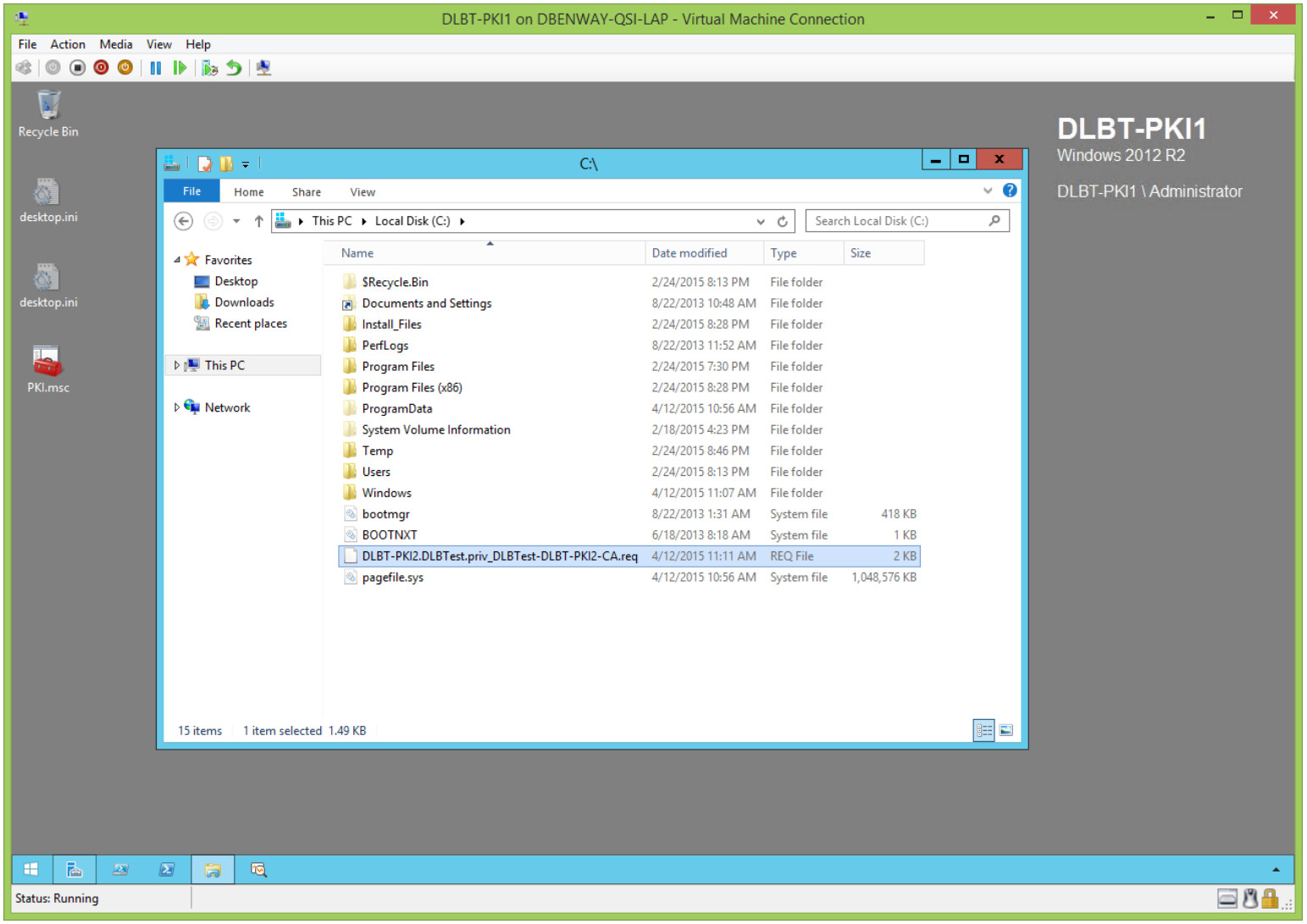
Sub/Policy/Issuing CA's Certificate Request (Before CertUtil.exe):

(jump to TOC)

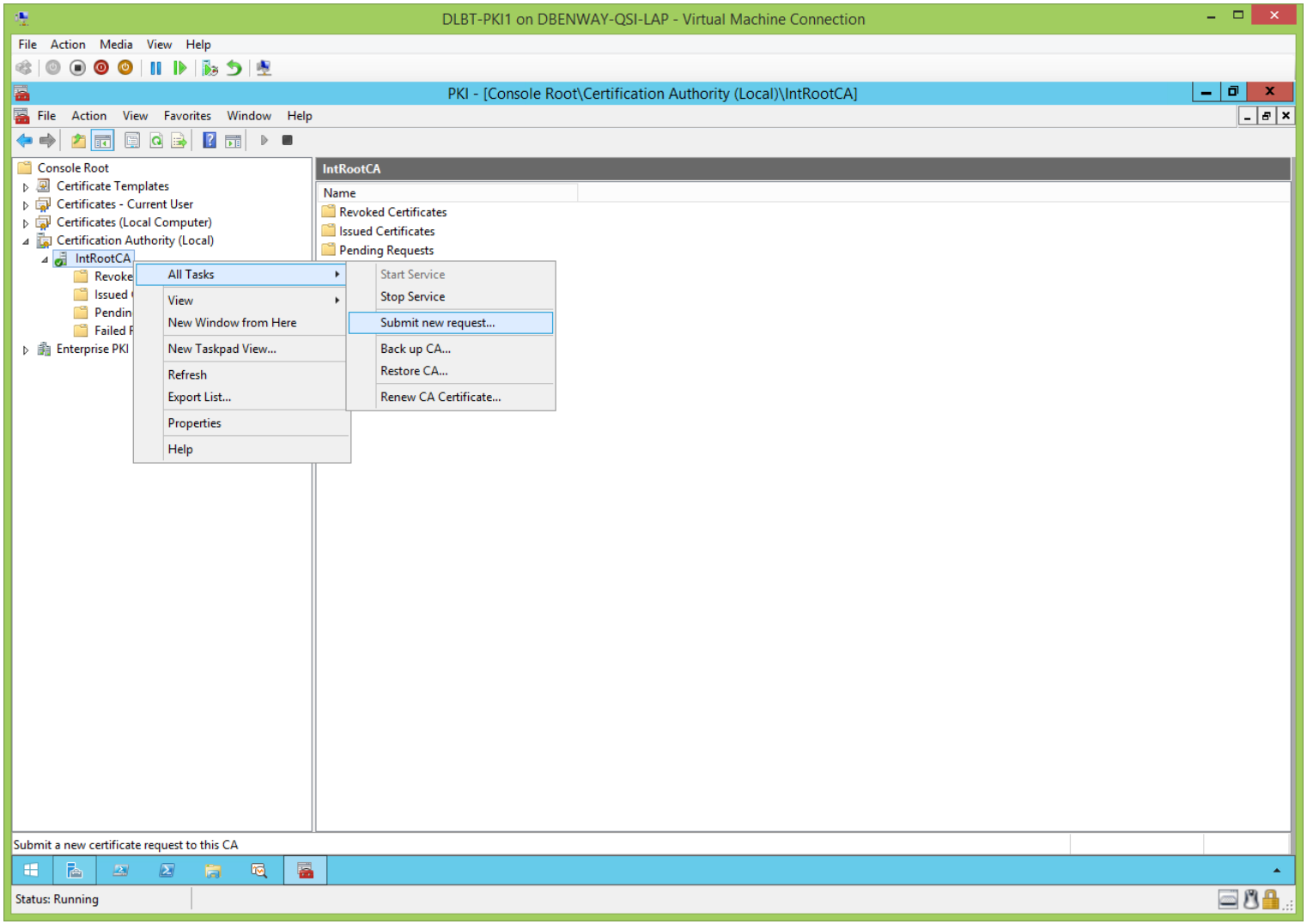
Use a thumb drive to copy the certificate request file (.req) from the sub/policy/issuing CA to the root CA:



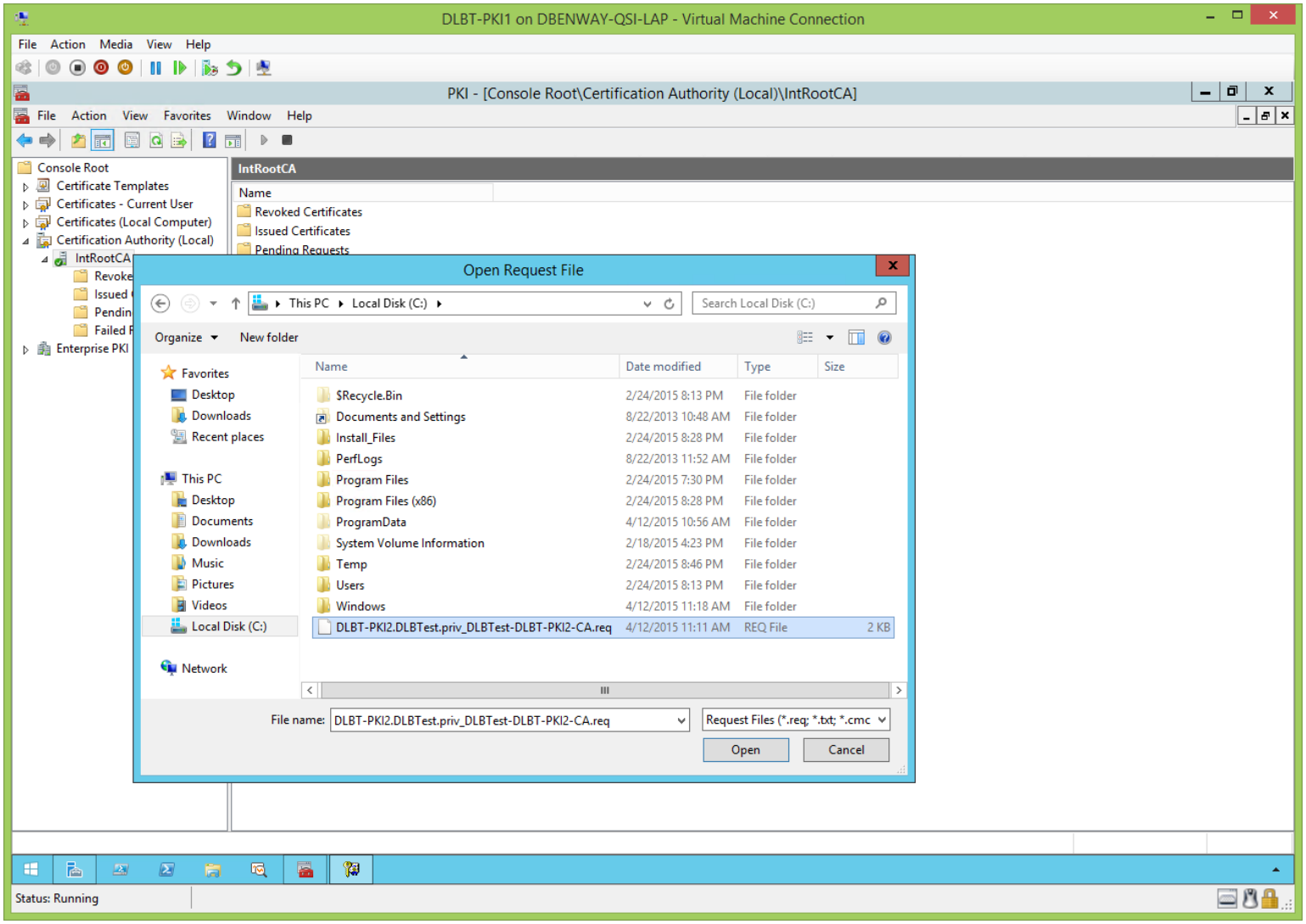
Here's the certificate request file (.req) on the root CA, copied from the sub/policy/issuing CA:



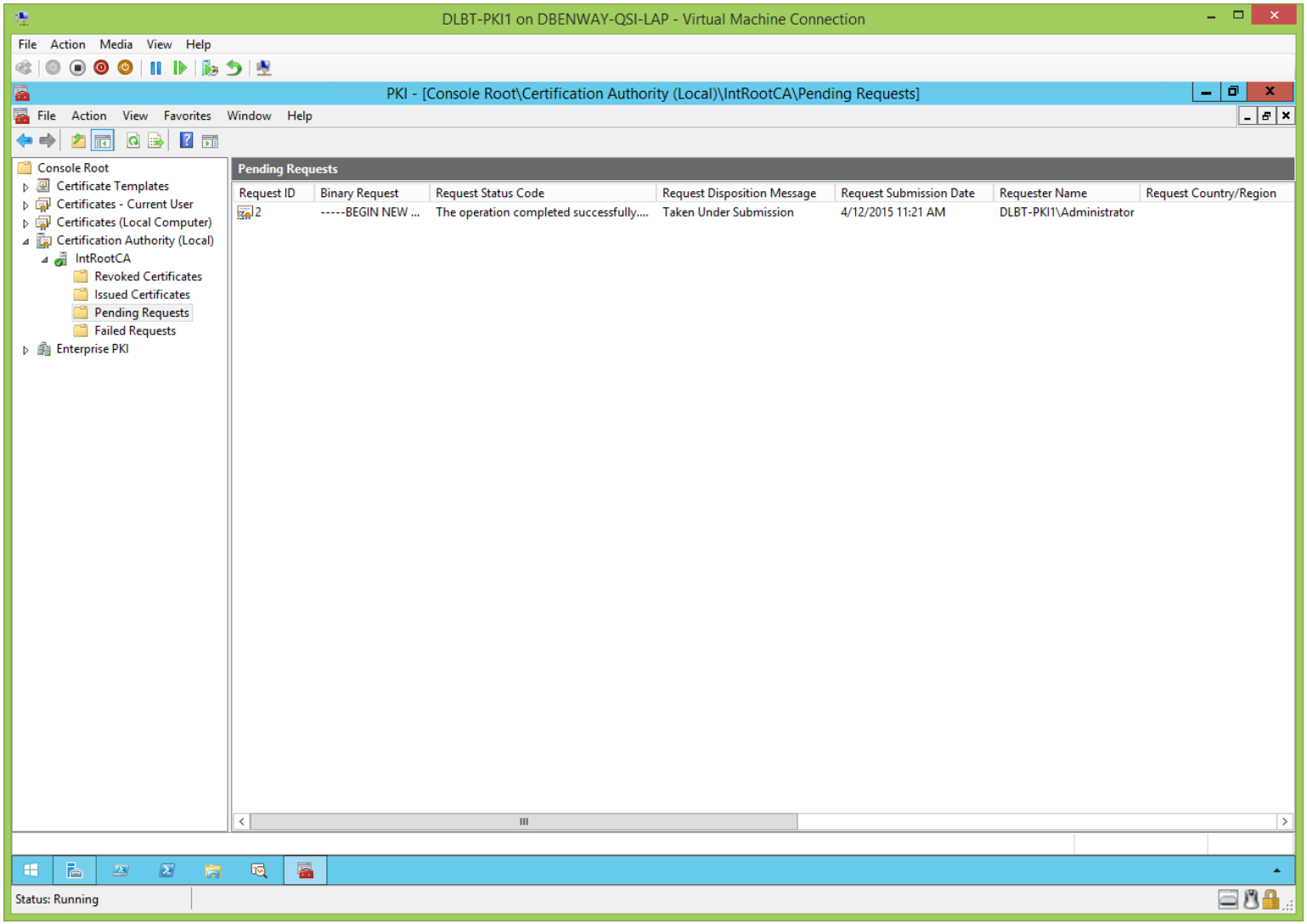
On the root CA, submit the sub/policy/issuing CA's certificate request by pointing to the local copy of the certificate request (.req) file:



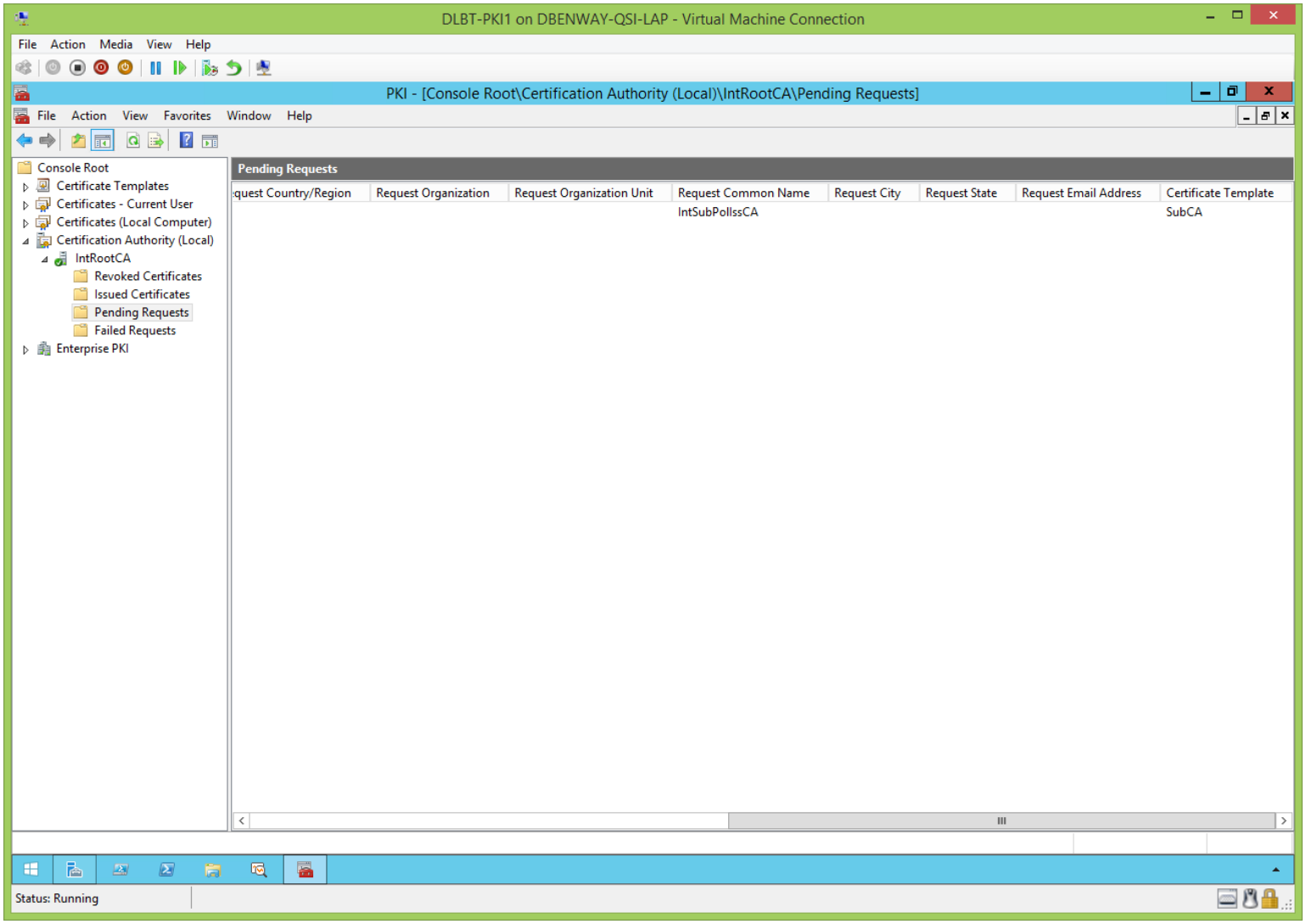
On the root CA, submit the sub/policy/issuing CA's certificate request by pointing to the local copy of the certificate request (.req) file:



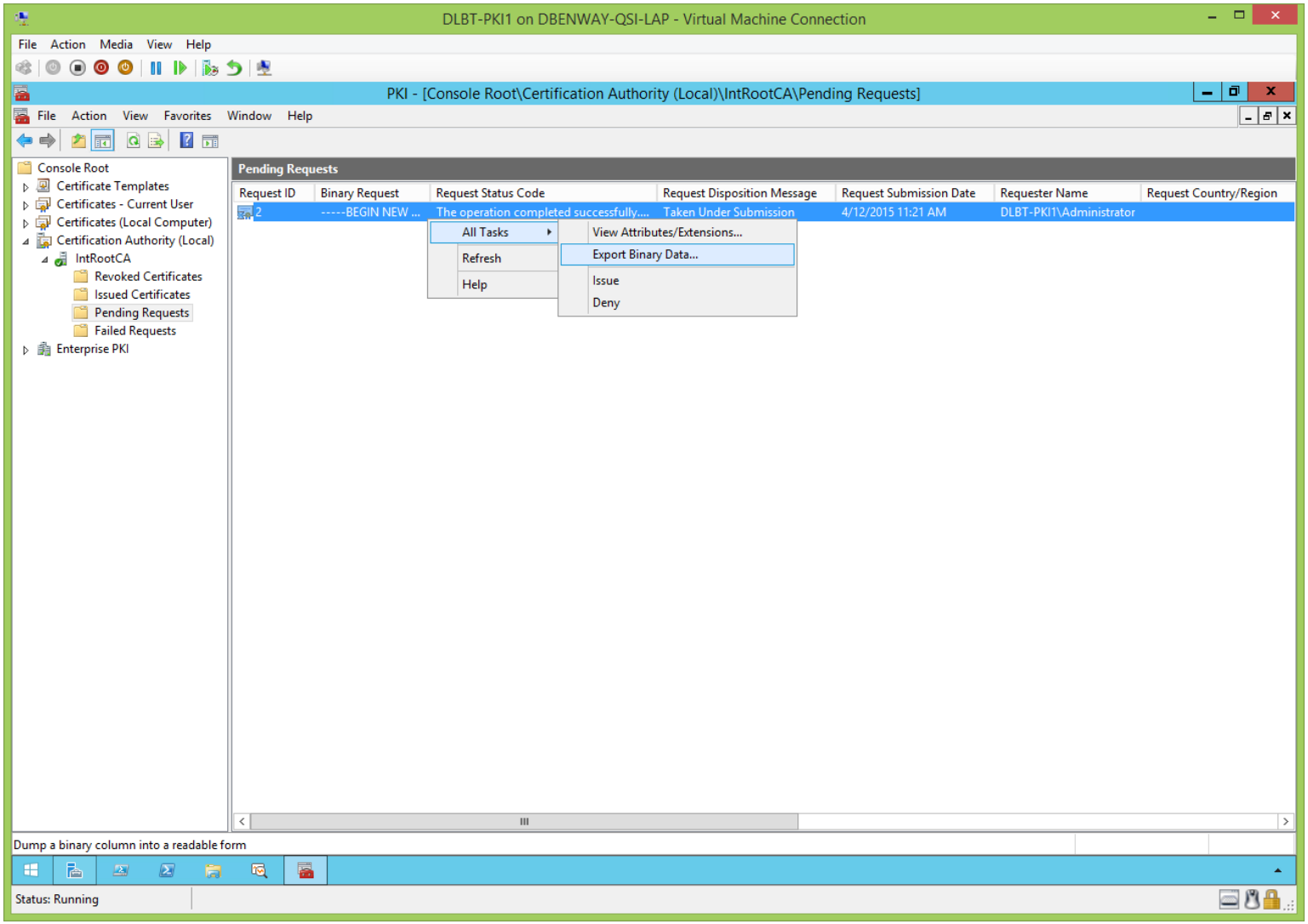
The sub/policy/issuing CA's pending certificate request appears on the root CA:



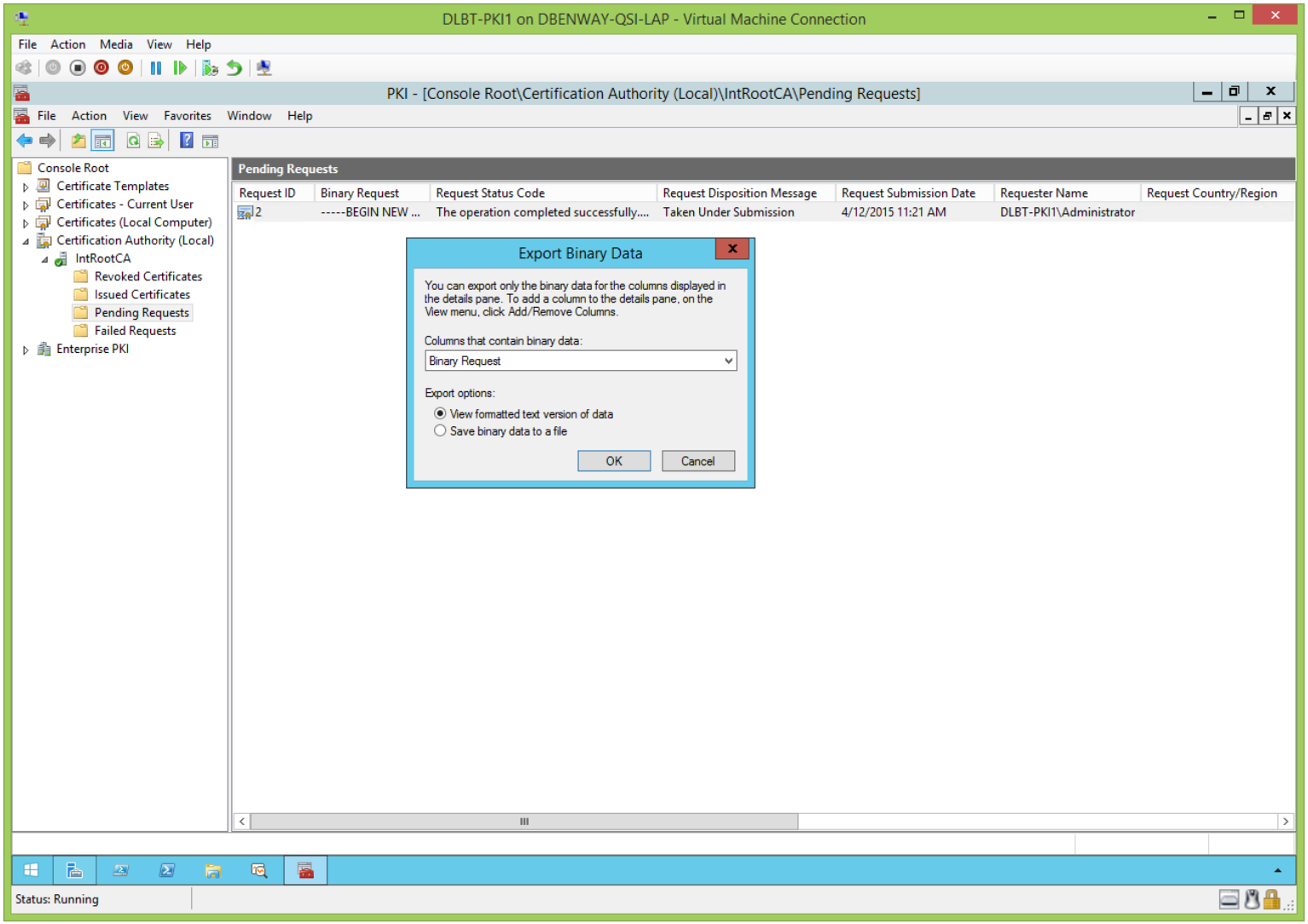
The sub/policy/issuing CA's pending certificate request appears on the root CA, cont'd:



RC the pending request > All Tasks > Export Binary Data:



Change ‘Columns that contain binary data:’ to ‘Binary Request’, click OK to view the formatted text version of the data:



Review the data in the pending request, then close the window:

DLBT-PKI1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

PKI - [Console Root\Certification Authority (Local)\IntRootCA\Pending Requests]

File Action View Favorites Window Help

Console Root
- Certificate Templates
- Certificates - Current User
- Certificates (Local Computer)
- Certification Authority (Local)
  - IntRootCA
    - Revoked Certificate
    - Issued Certificates
    - Pending Requests
    - Failed Requests
- Enterprise PKI

Pending Requests

Request ID	Binary Request	Request Status Code	Request Disposition Message	Request Submission Date	Requester Name	Request Country/Region
2	-----BEGIN NEW ...	The operation completed successfully....	Taken Under Submission	4/12/2015 11:21 AM	DLBT-PKI1\Administrator	

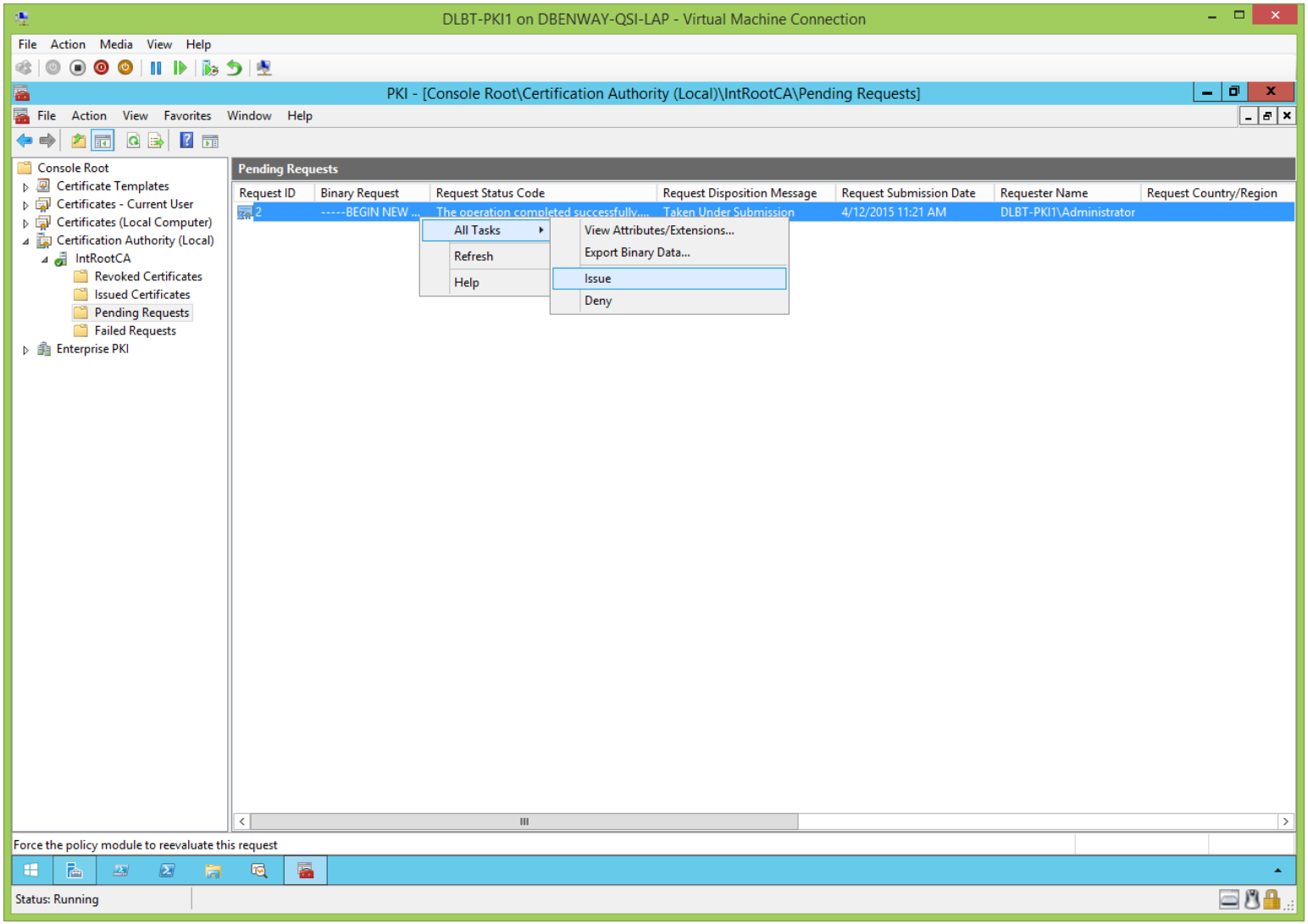
Binary Request - 2.tmp - Notepad

File Edit Format View Help

```
PKCS10 Certificate Request:
Version: 1
Subject:
    CN=IntSubPolIssCA
    DC=DLBTest
    DC=priv
  Name Hash(sha1): 65776ce60eb8402c9d1e933c1d44dfef2b6be501
  Name Hash(md5): 173f382699445f8c0b00d15f4dd26021

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 2048 bits
Public Key: UnusedBits = 0
    0000  30 82 01 0a 02 82 01 01  00 db 1c ea 68 ca 6a 6b
    0010  c5 87 84 2d 78 68 94 75  22 b9 30 90 0c 72 ea 2b
    0020  d2 f9 7d 80 76 8f 68 99  ba 67 ea 4d 89 63 74 e4
    0030  b4 26 3c 61 54 56 cc ac  df 91 71 93 1a 11 3f b5
    0040  94 0f d1 87 a1 e2 44 fc  f8 17 c8 03 9a 14 bf 4f
    0050  9d b1 58 2e 82 b0 98 b3  96 b3 1a 50 2b 64 01 6d
    0060  6c a8 8a 6b ef 18 7f 06  67 57 ff 8a 07 d6 93 78
    0070  0f 2b 7f c1 67 b6 54 bd  e4 59 68 ca 04 9b a3 1e
    0080  4d 14 31 7b cf 04 00 a3  b2 92 e4 11 40 f2 c5 51
    0090  f5 af e1 57 b7 8b f6 6d  61 78 eb d0 4c d4 3f 6b
    00a0  d3 18 c5 6e 1c cf 43 fa  e7 d7 0e a7 a9 2e 68 45
```

Status: Running

Issue the certificate from the root CA for the sub/policy/issuing CA:



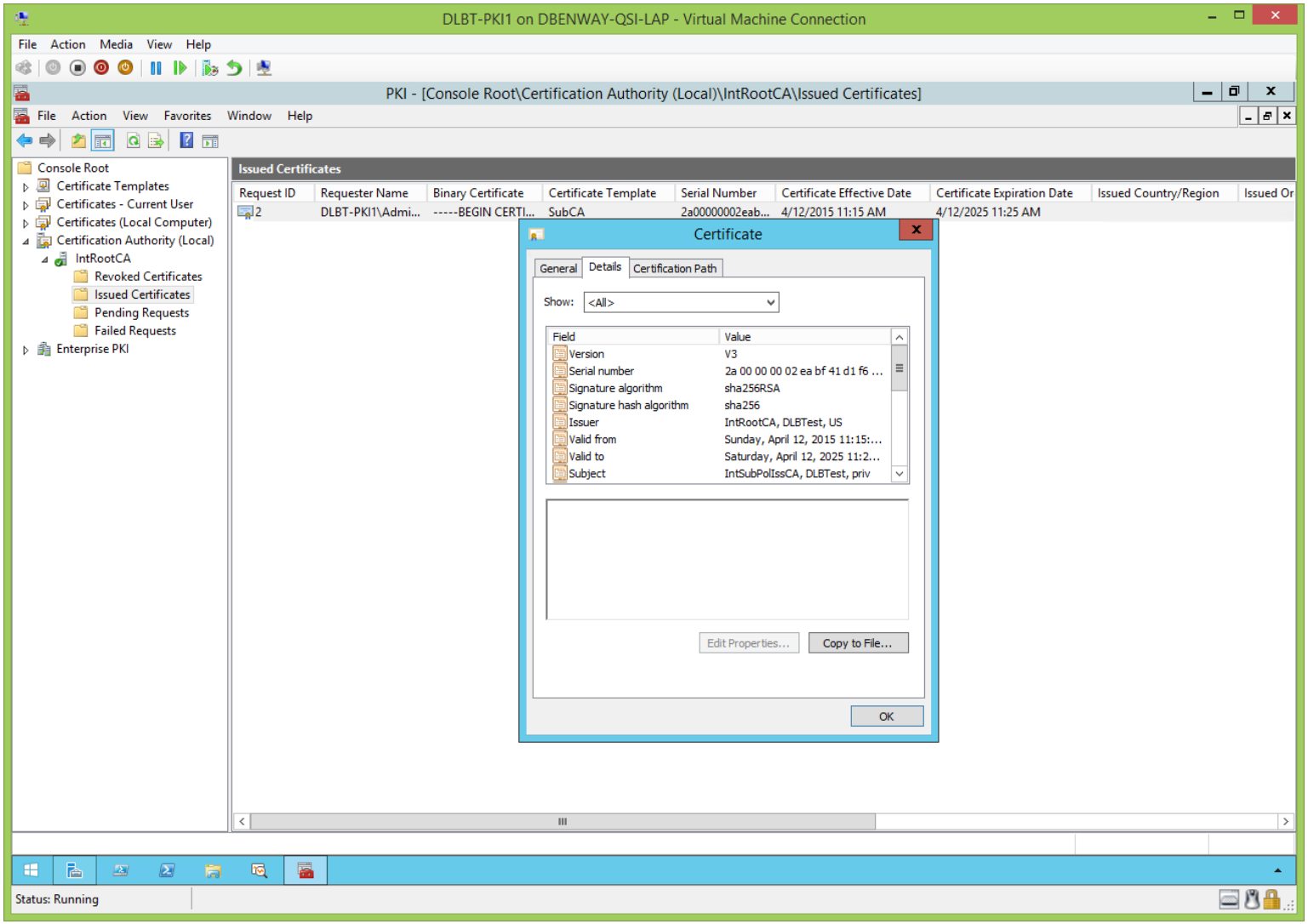
Now that the root CA has issued a new certificate for the sub/policy/issuing CA, publish the root CA's CRL (to whatever the root CA's CDP extensions specify) by using certUtil.exe:

- certUtil.exe –CRL

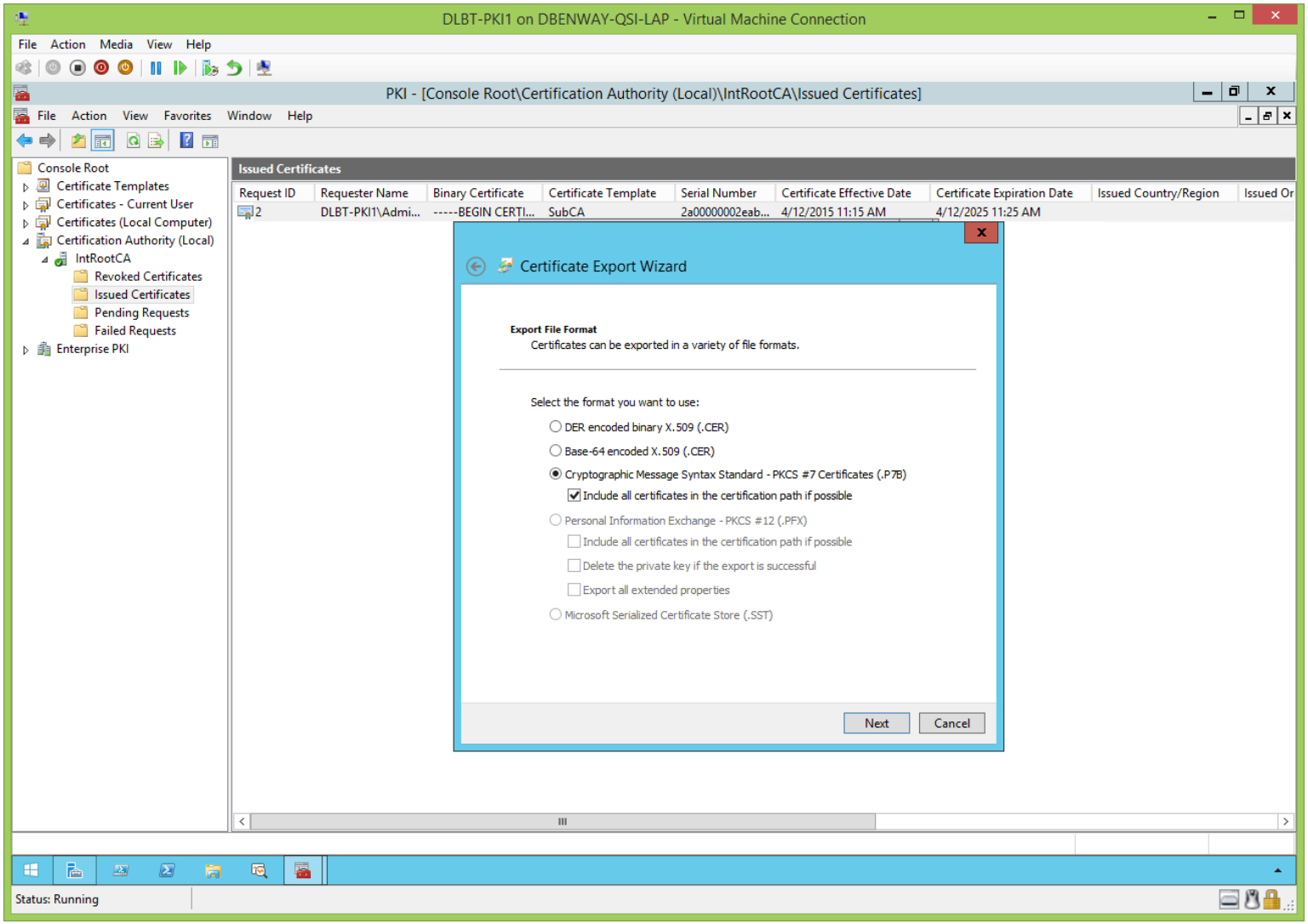
Now that the root CA has published a new CRL, copy it to the CDP via a thumb drive.

- copy the root CA's %windir%\system32\CertSrv\CertEnroll*.crl to the CDP's C:\IntePub\PKI\CDP

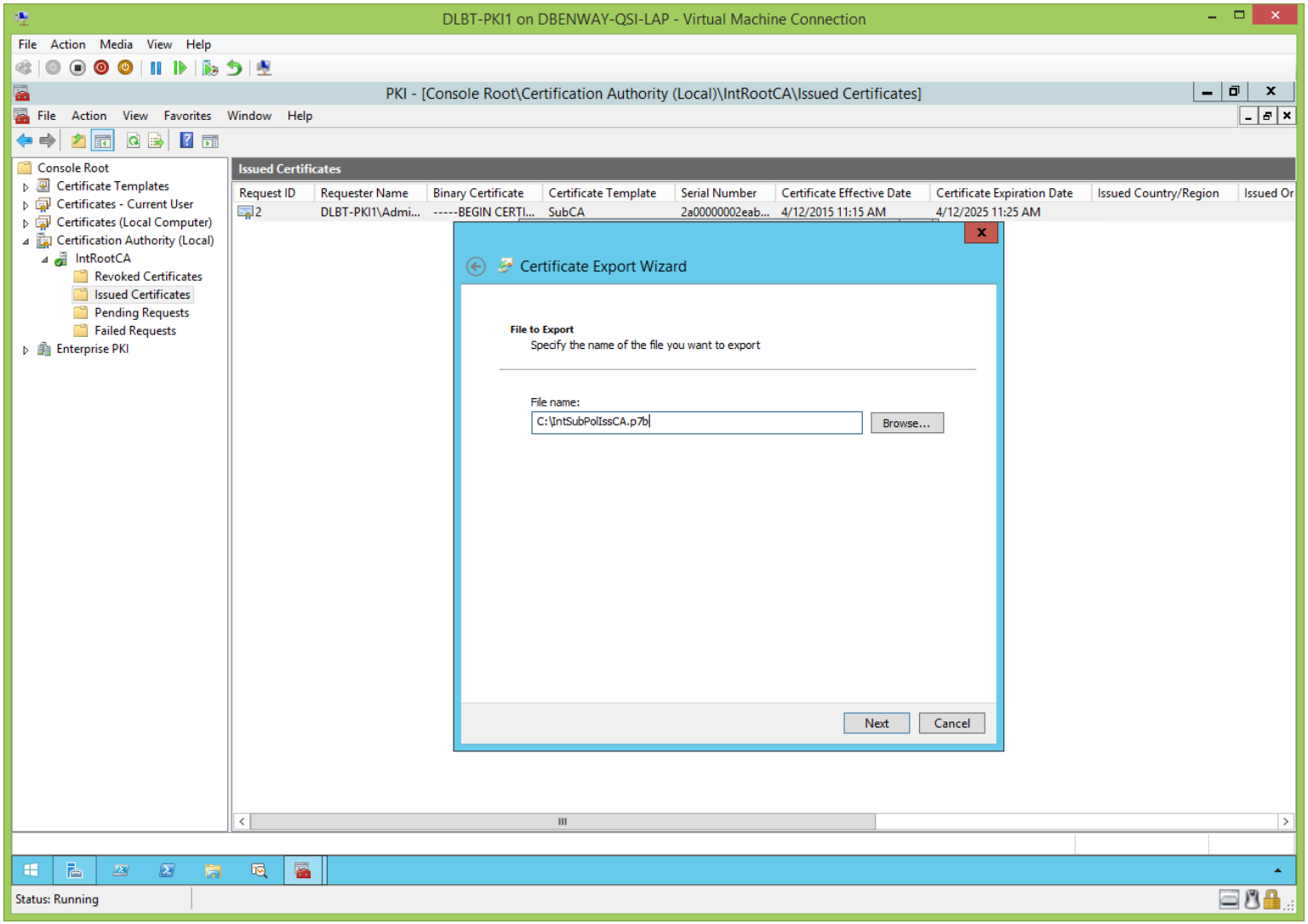
Copy the issued sub/policy/issued CA's certificate from the root CA to a file which can be brought to the sub/policy/issuing CA.
LCC the issued certificate > Details > Copy to File… :



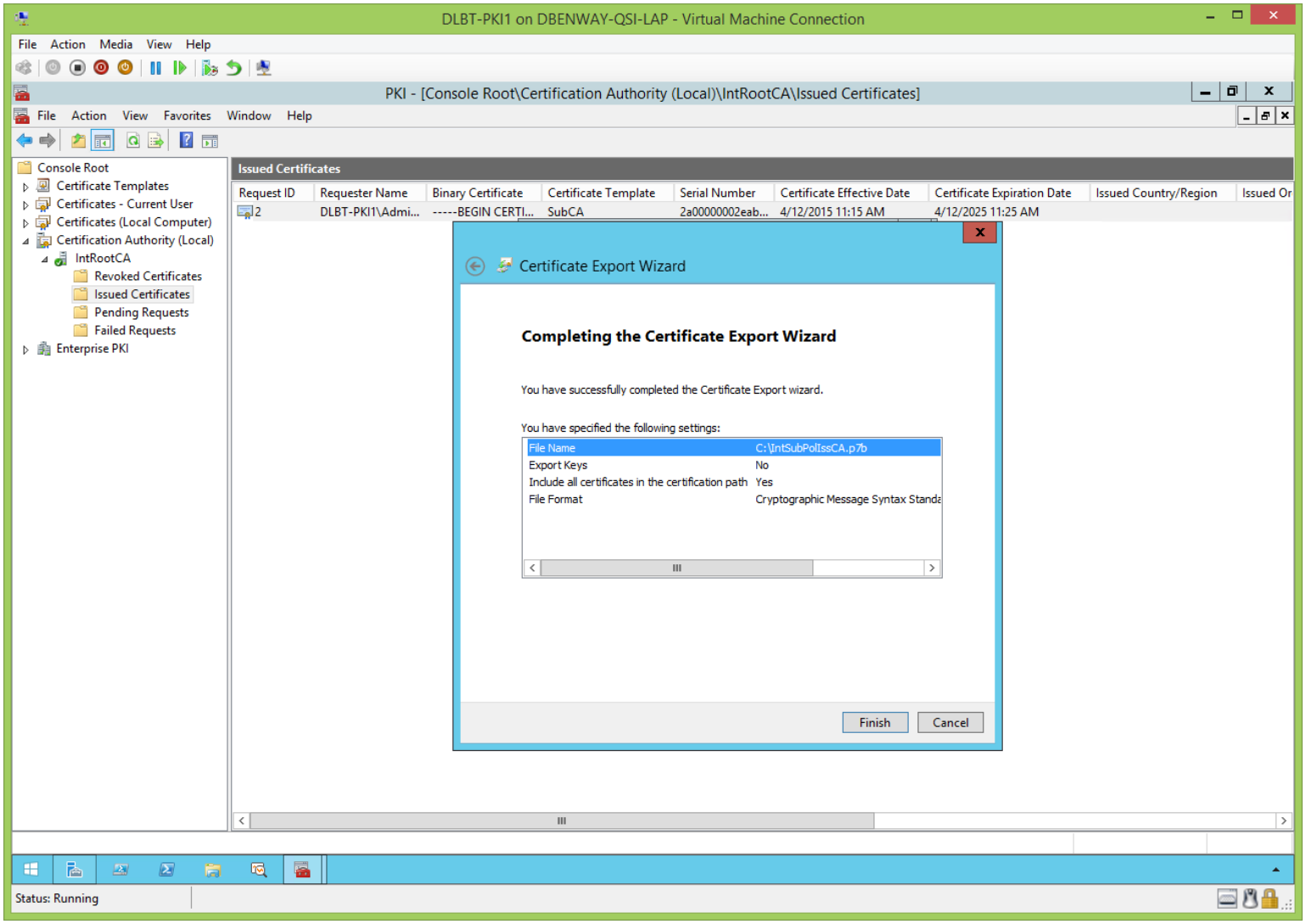
Choose PKCS #7, and include all certificates in the certification path if possible:



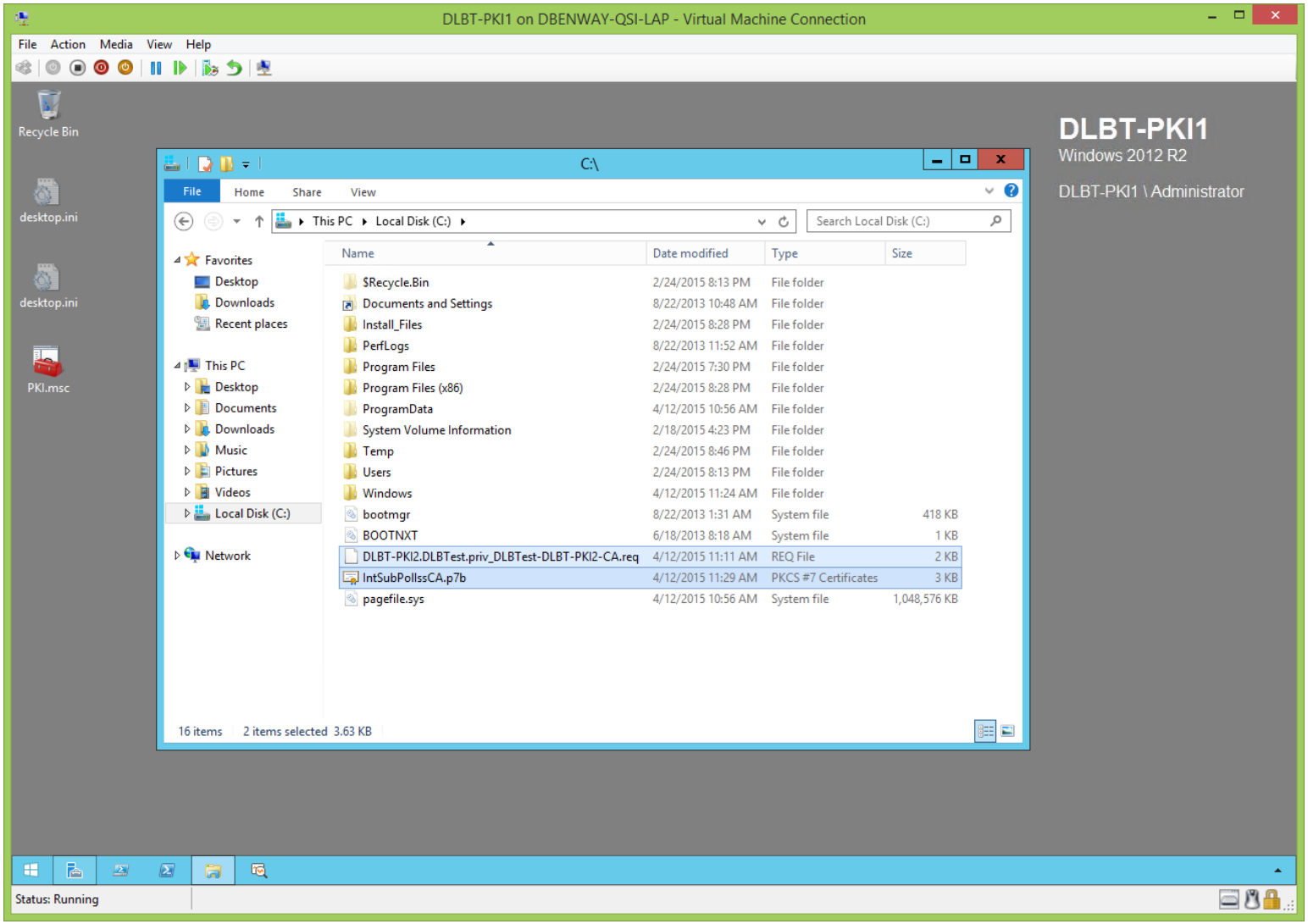
Specify a path and name for the sub/policy/issuing CA's certificate to be copied to (use a 'p7b' extension):



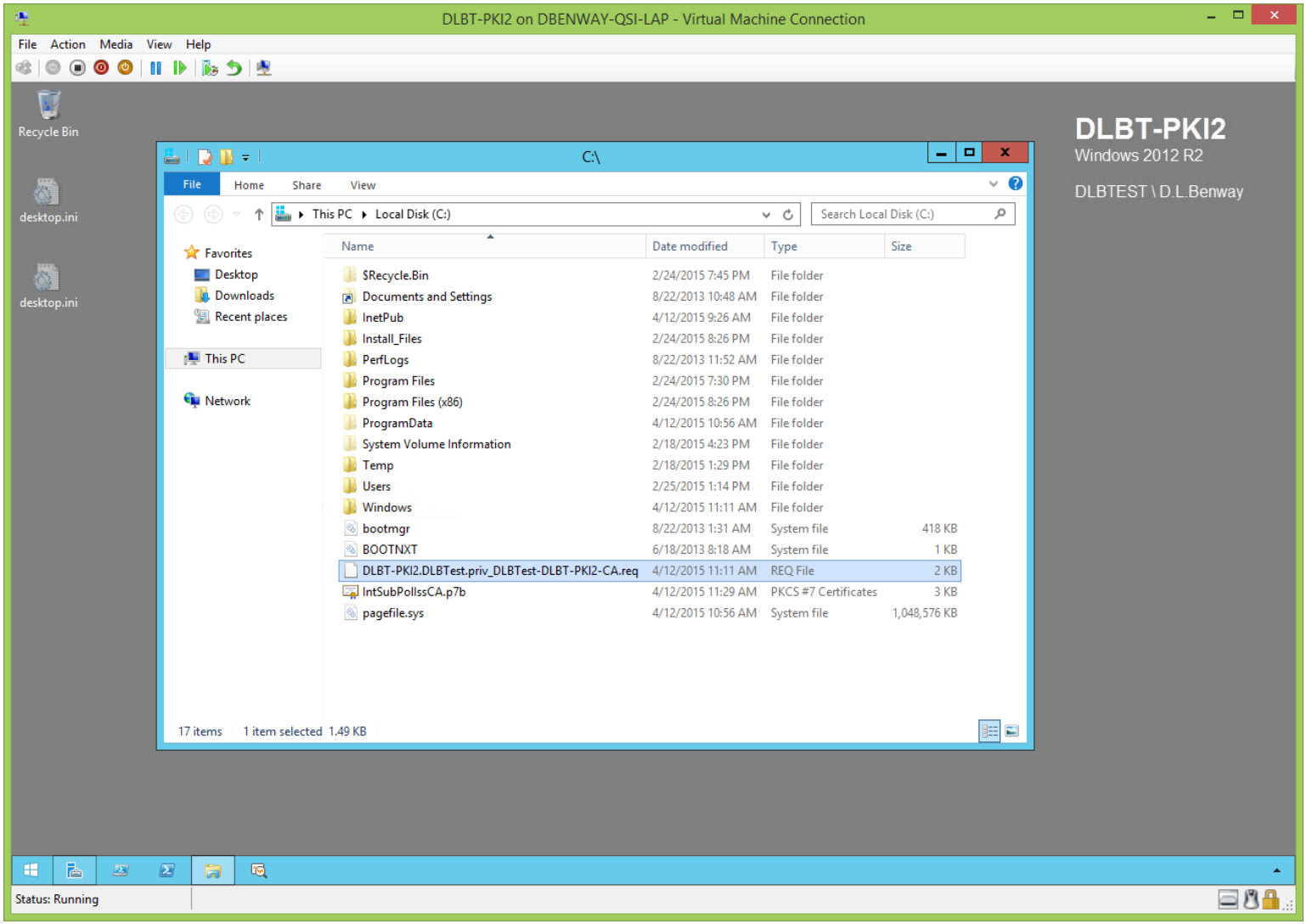
Finish the wizard:



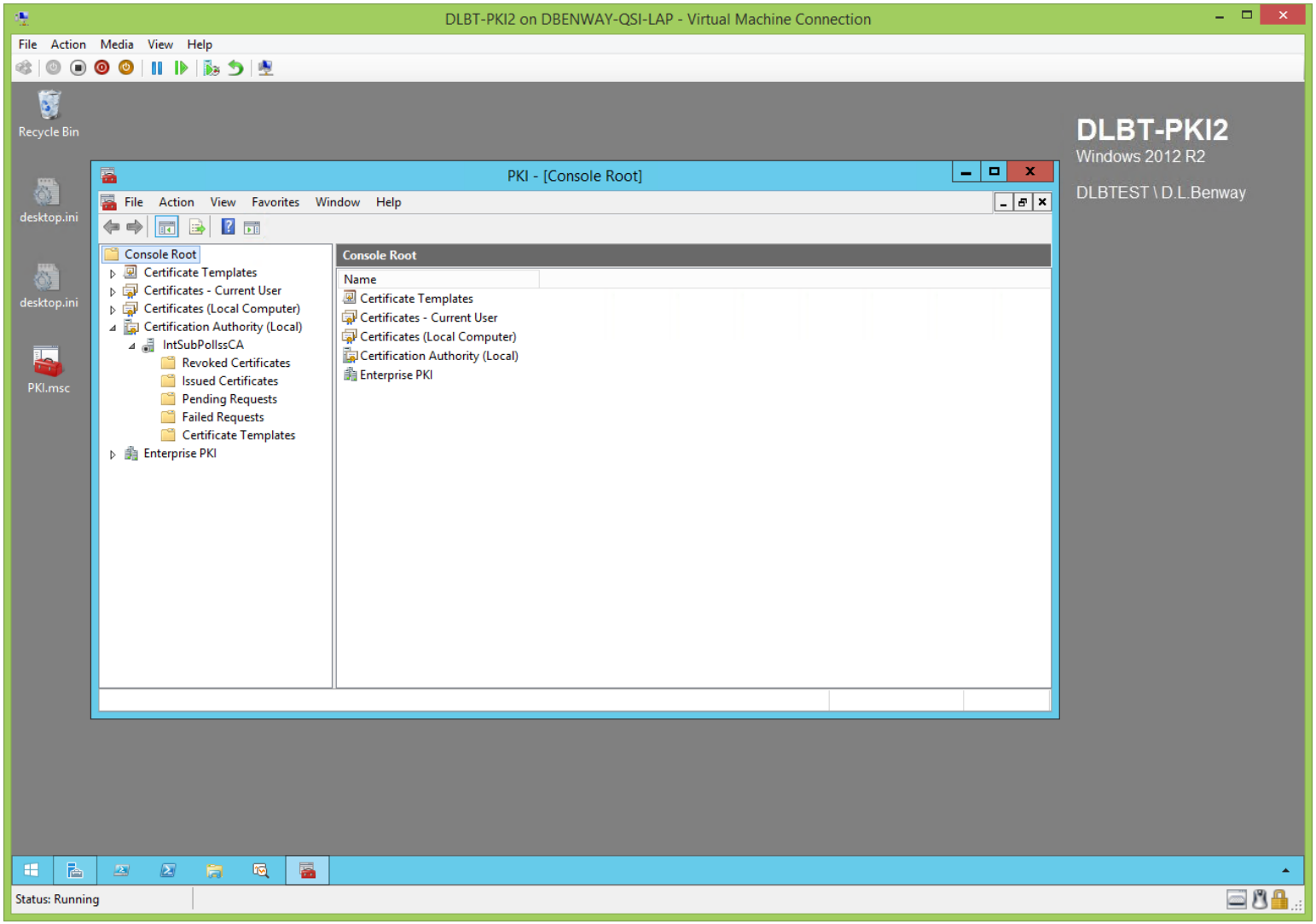
Delete the sub/policy/issuing CA's certificate request off of the root CA, and use a thumb drive to move the newly issued sub/policy/issuing CA's certificate from the root CA to the sub/policy/issuing CA:



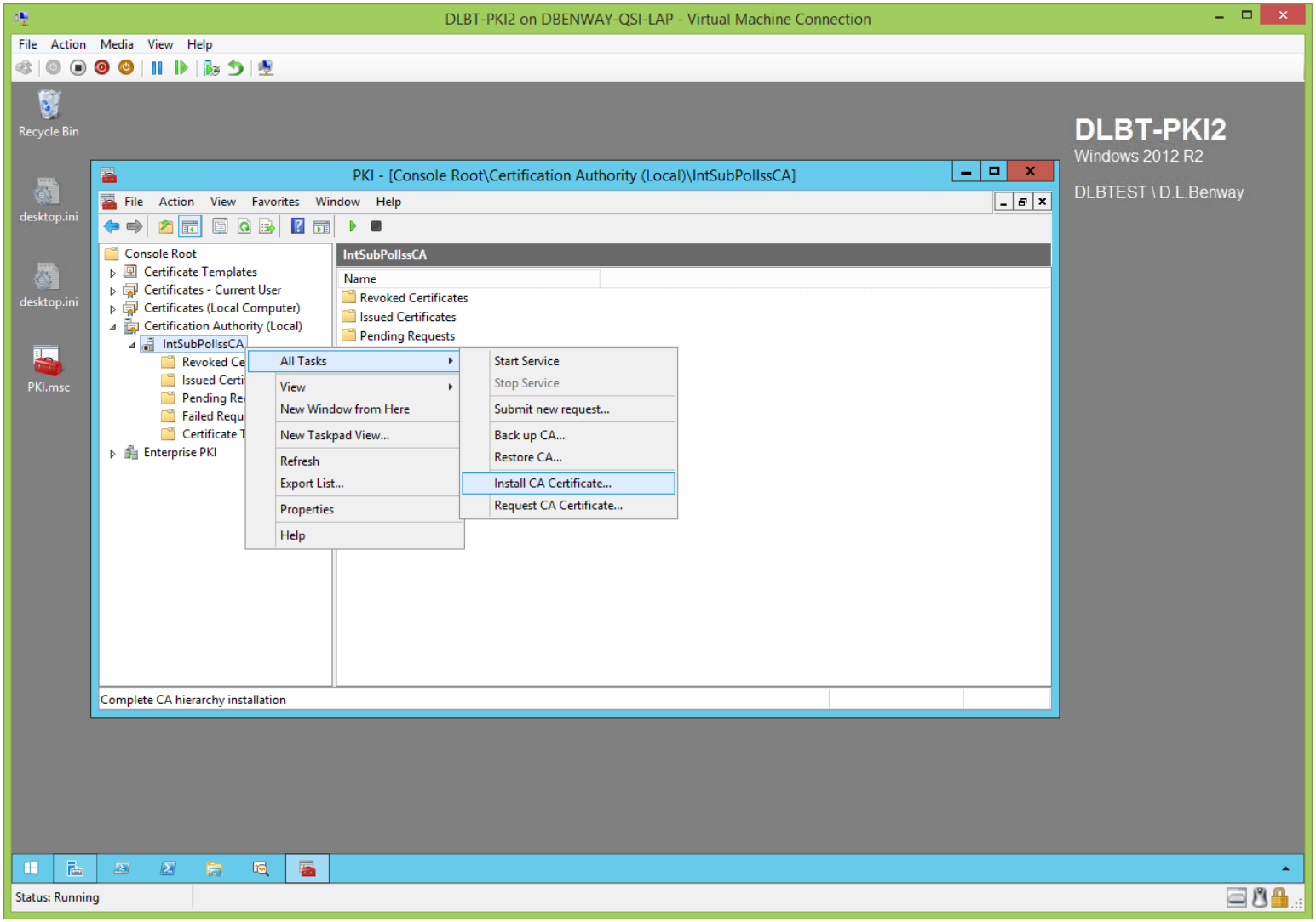
Delete the sub/policy/issuing CA's certificate request off of the sub/policy/issuing CA:



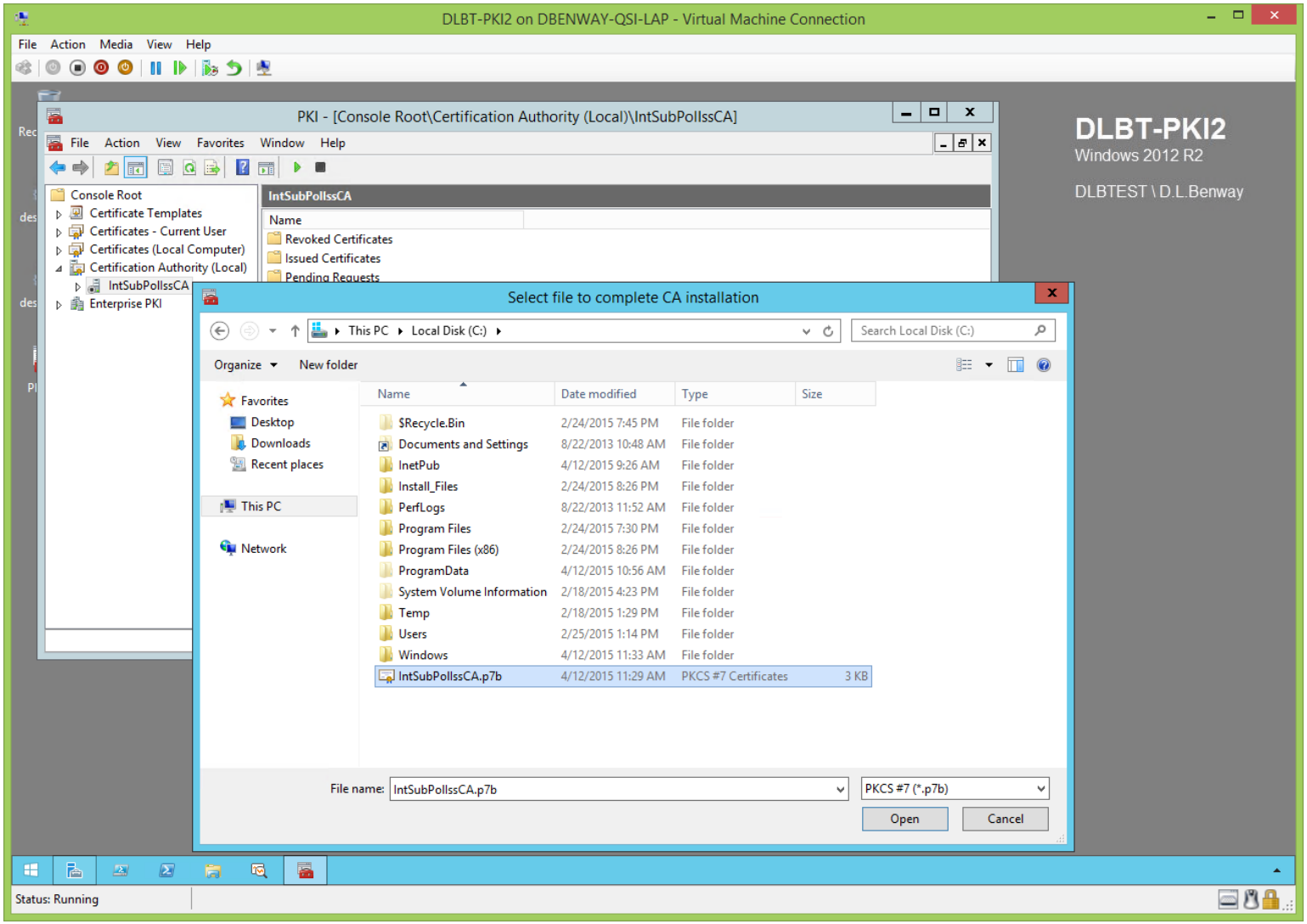
Create and save the sub/policy/issuing CA's PKI MMC, just like how we created and saved the root CA's PKI MMC:



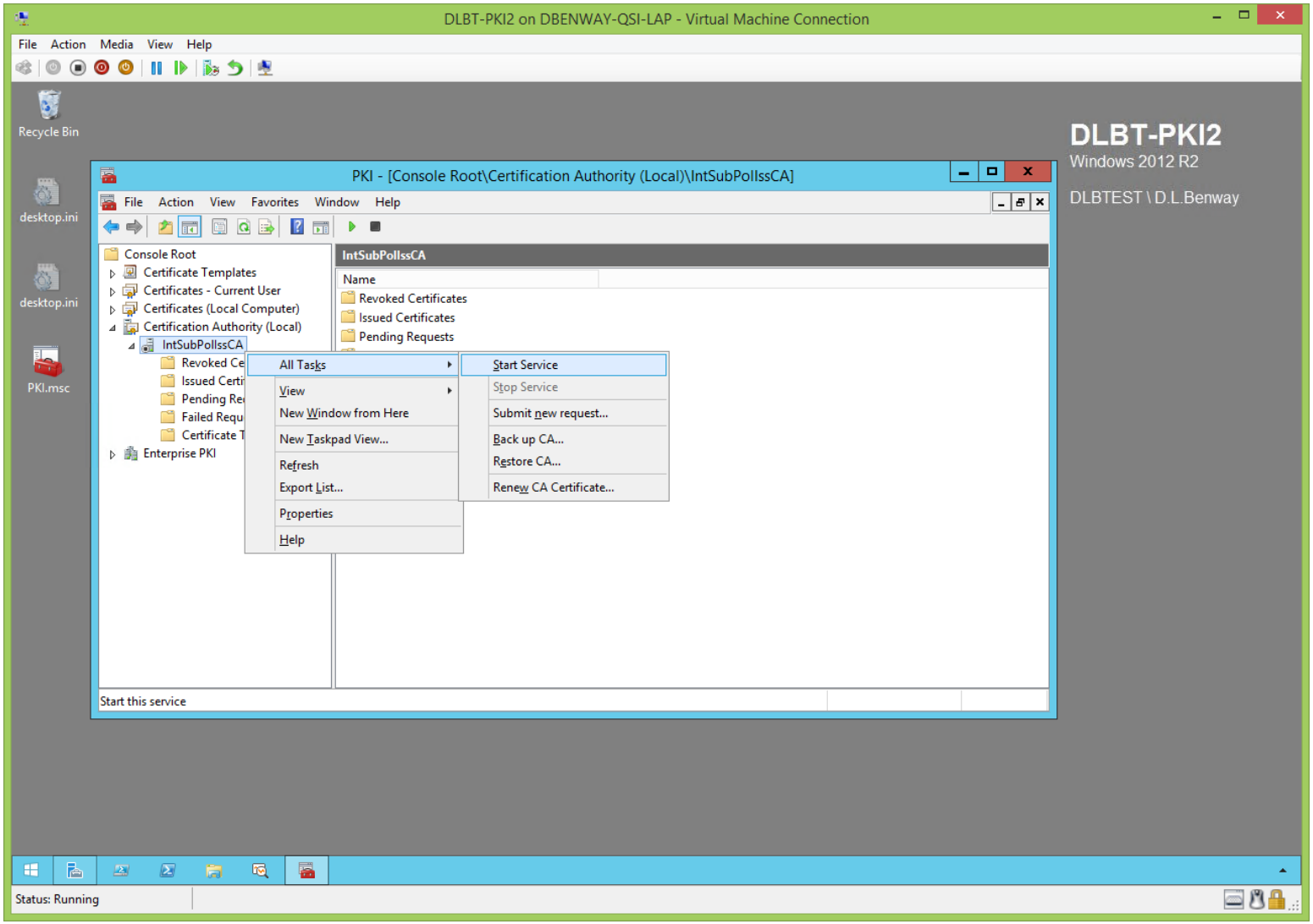
Install the copied sub/policy/issuing CA's certificate onto the sub/policy/issuing CA:



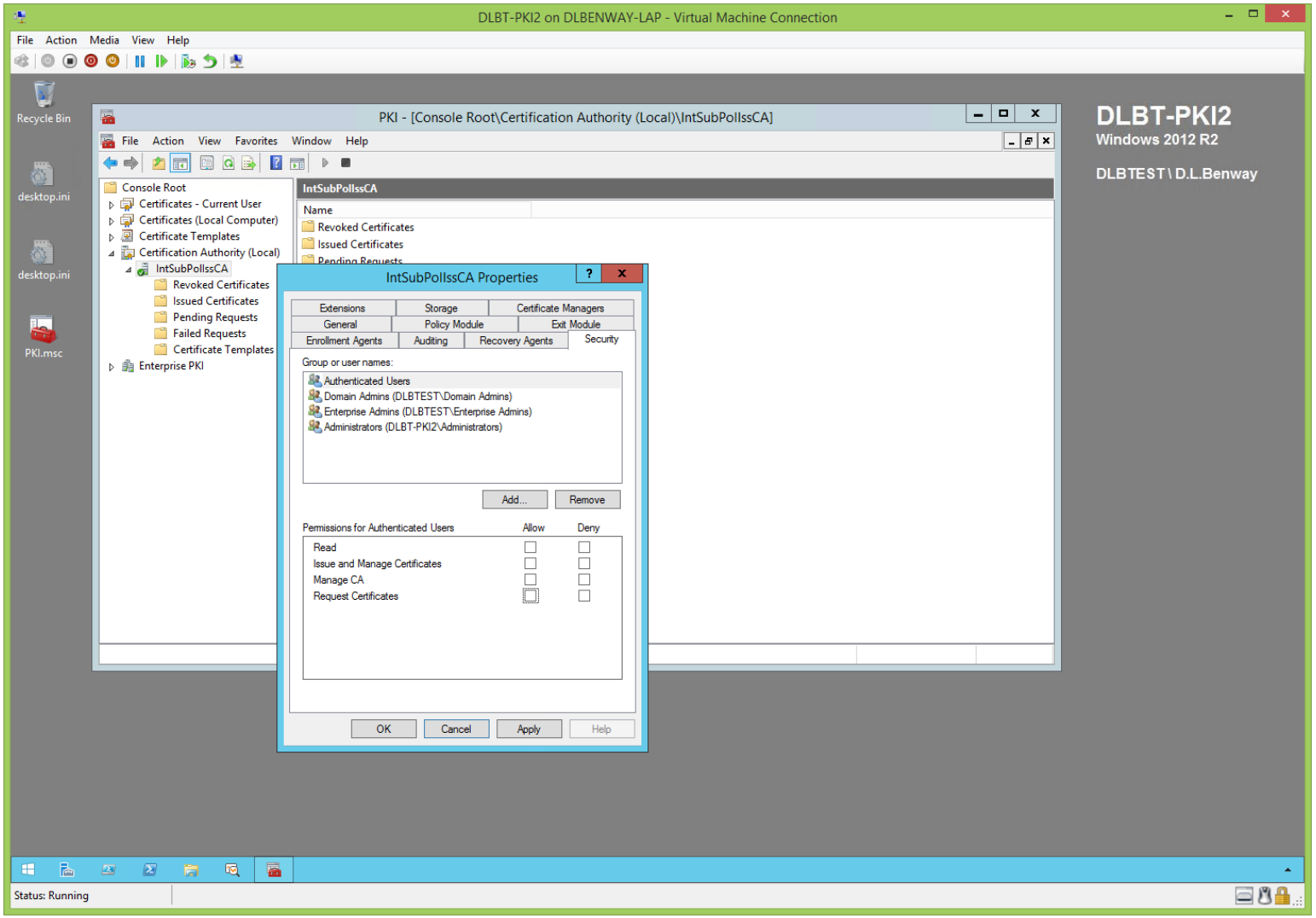
Choose the sub/policy/issuing CA's certificate that was copied from the root CA:



ADCS on the sub/policy/issuing CA will probably start automatically:

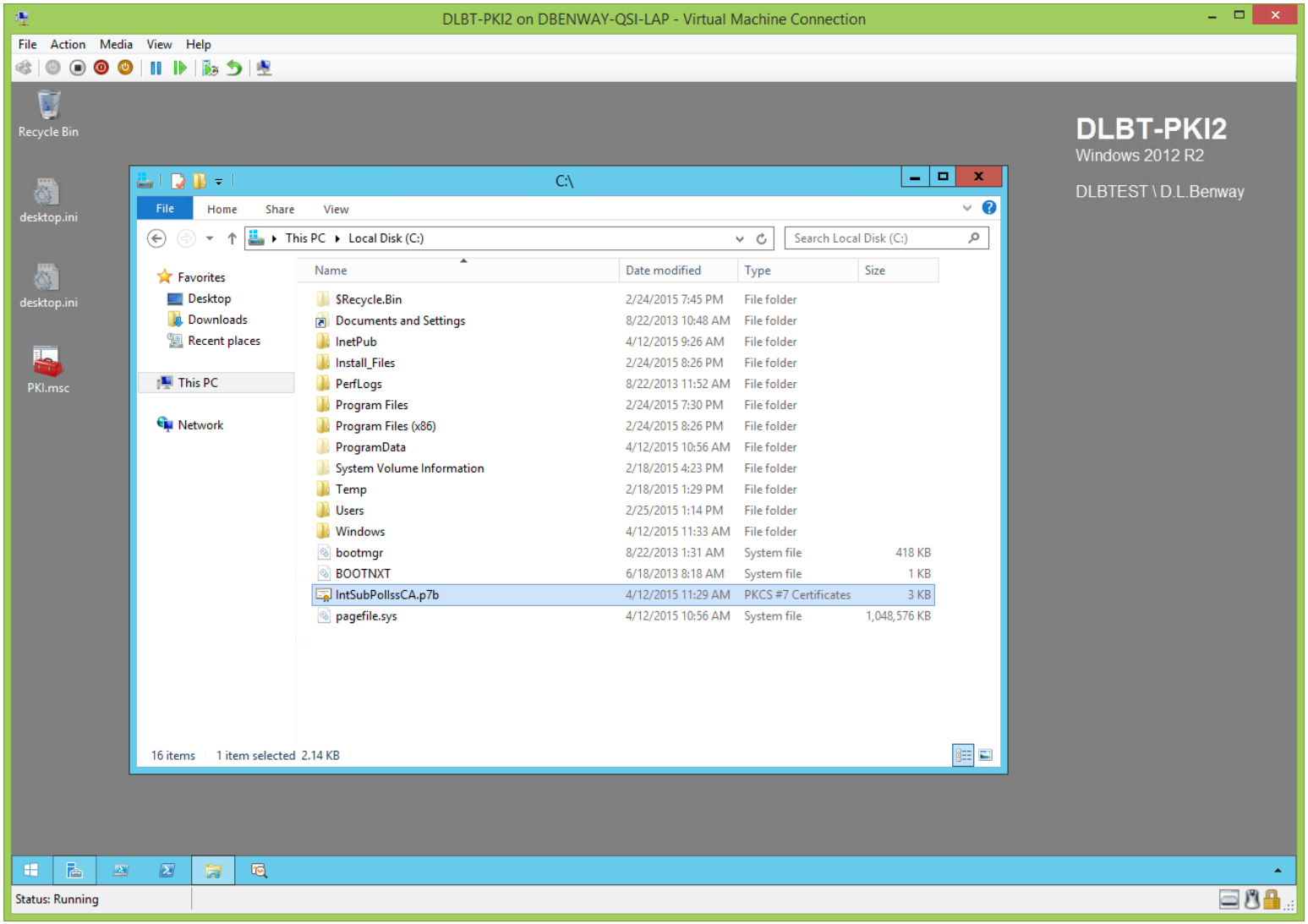


Temporarily prevent the sub/policy/issuing CA from issuing certificates (until it has been fully configured) by removing each group's and user's right on the CA to 'Request Certificates':



Note: the sub/policy/issuing CA will show up in Enterprise PKI as broken until you re-enable 'Authenticated Users' for requesting certificates.

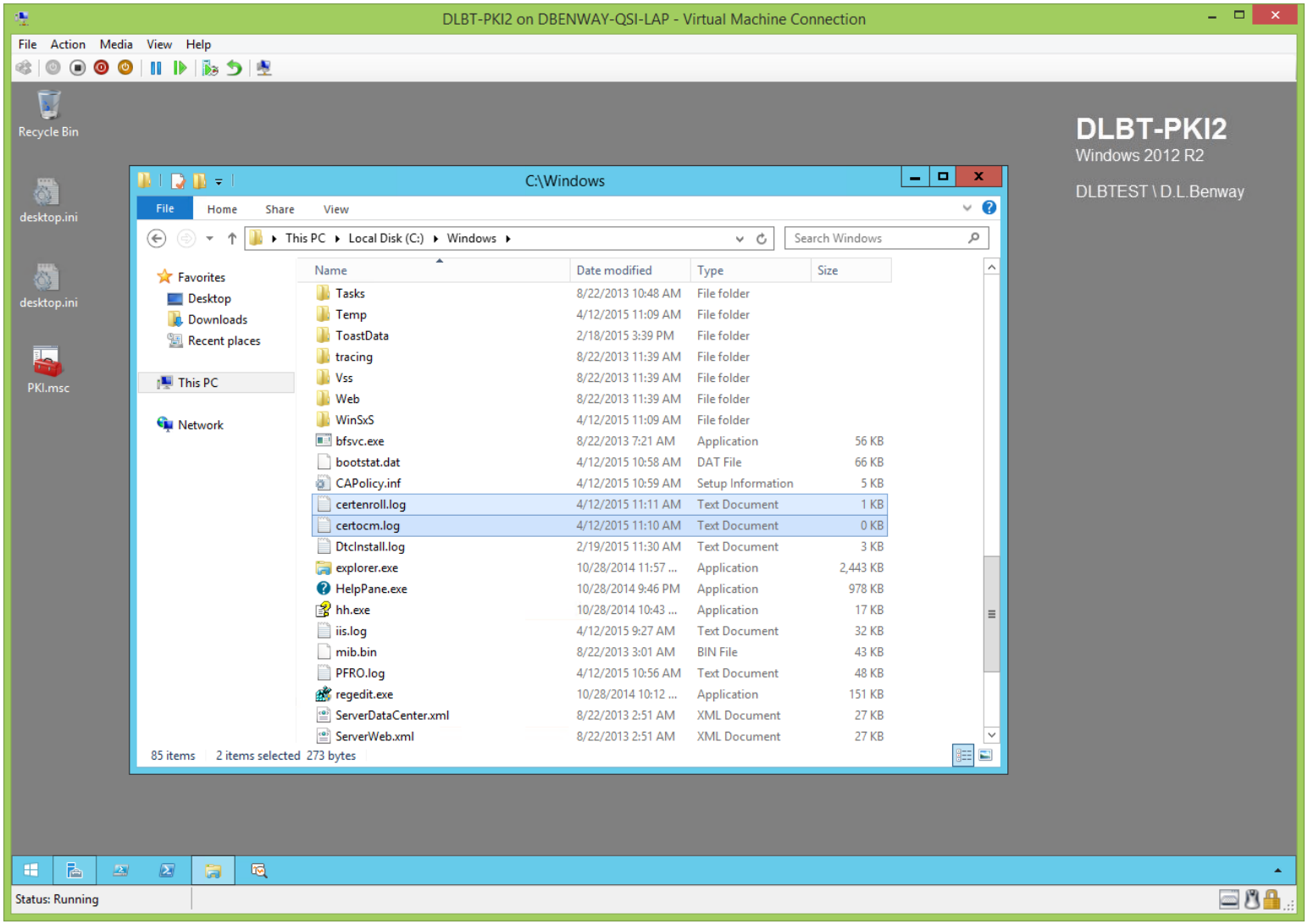
Delete the copied certificate off of the sub/policy/issuing CA:



Sub/Policy/Issuing CA's Logs (Before CertUtil.exe):

(jump to TOC)

You can view the log files, but they so carelessly use the words 'error' and 'fail' that I found them to be of limited value:



Sub/Policy/Issuing CA's PKI MMC (Before CertUtil.exe):

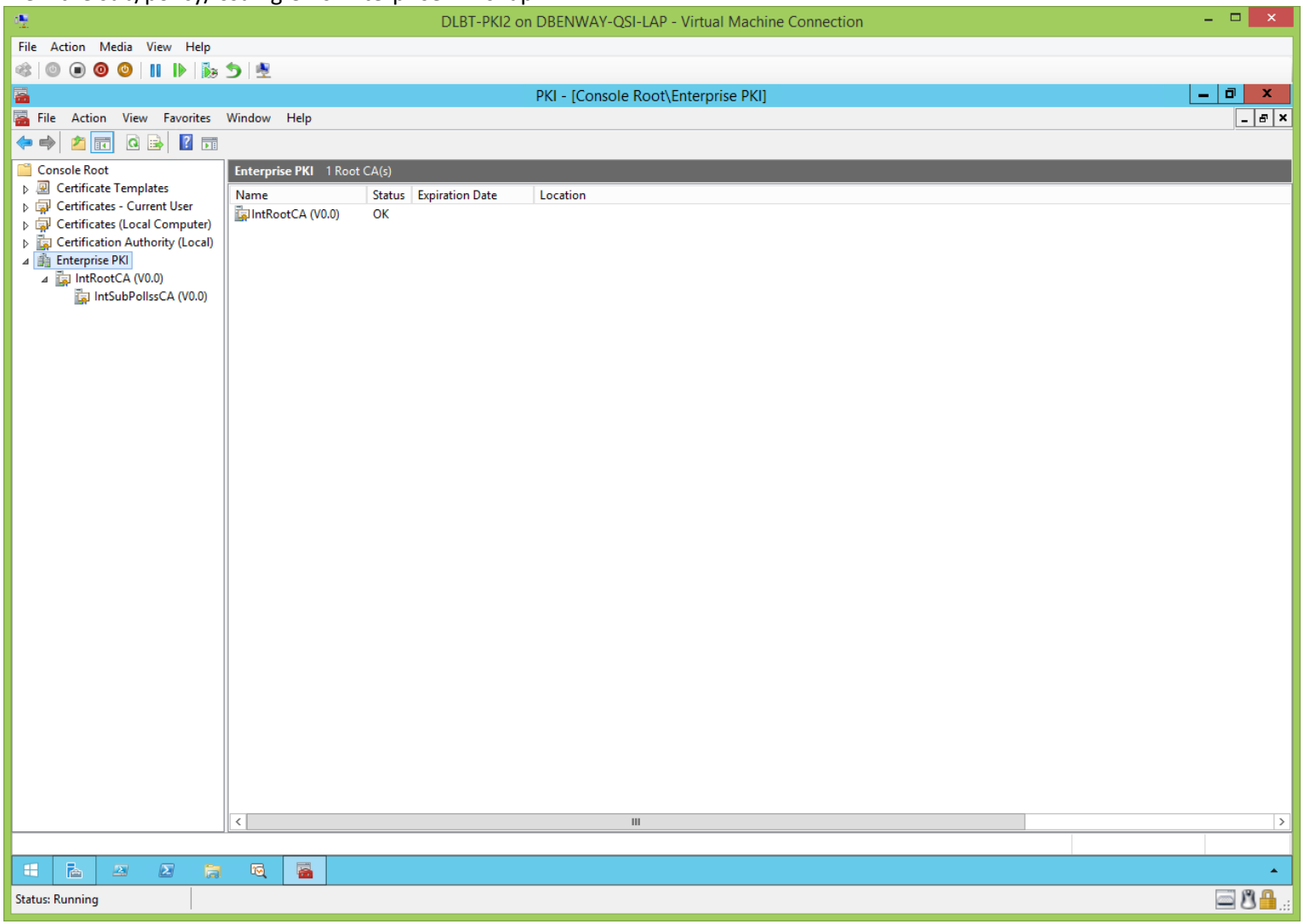
(jump to TOC)

This was already setup when we installed the sub/policy/issuing CA's certificate (which was created by the root CA) onto the sub/policy/issuing CA.

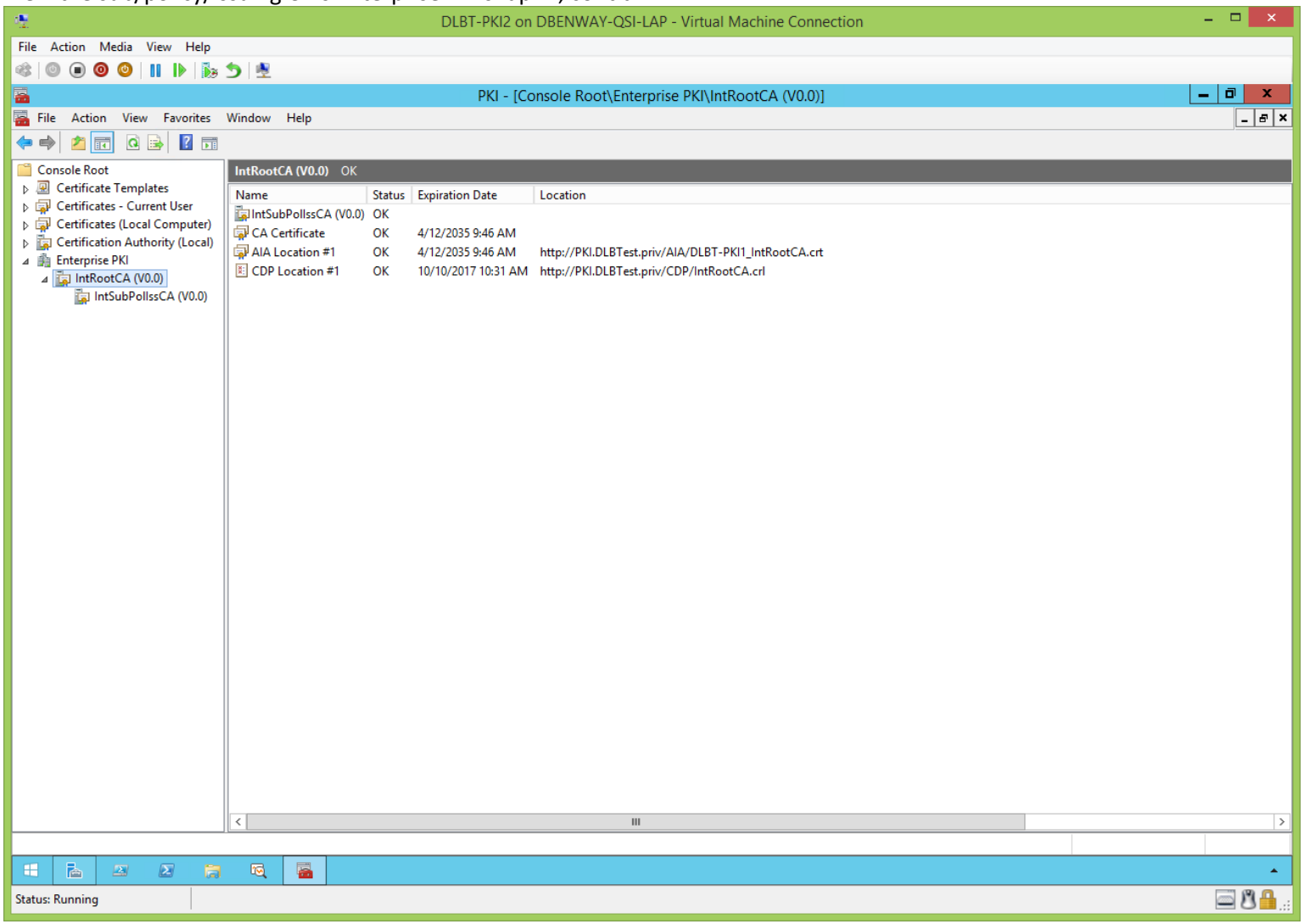
Sub/Policy/Issuing CA's Enterprise PKI Snap-In (Before CertUtil.exe):

(jump to TOC)

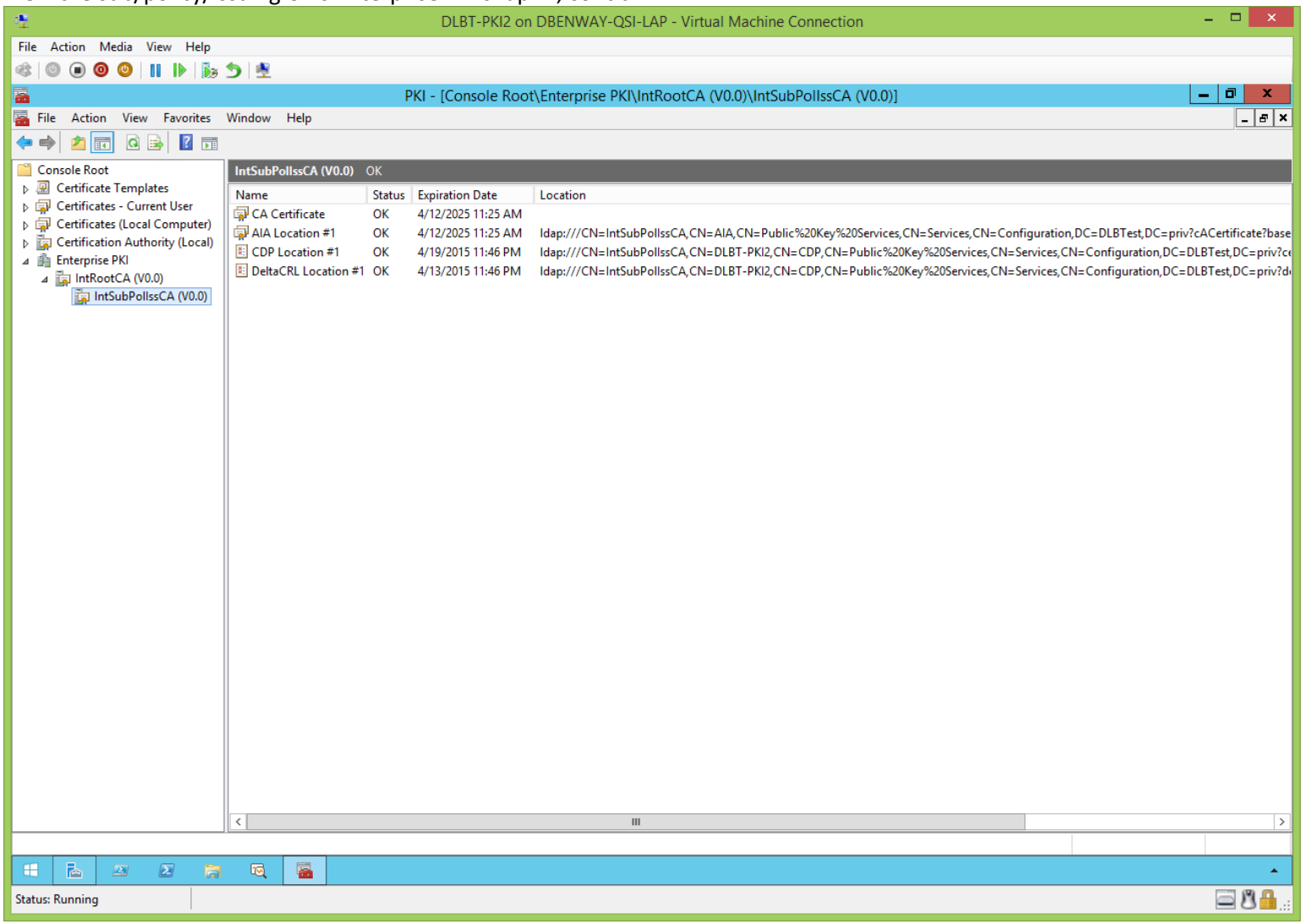
View the sub/policy/issuing CA's Enterprise PKI snap-in:



View the sub/policy/issuing CA's Enterprise PKI snap-in, cont'd:



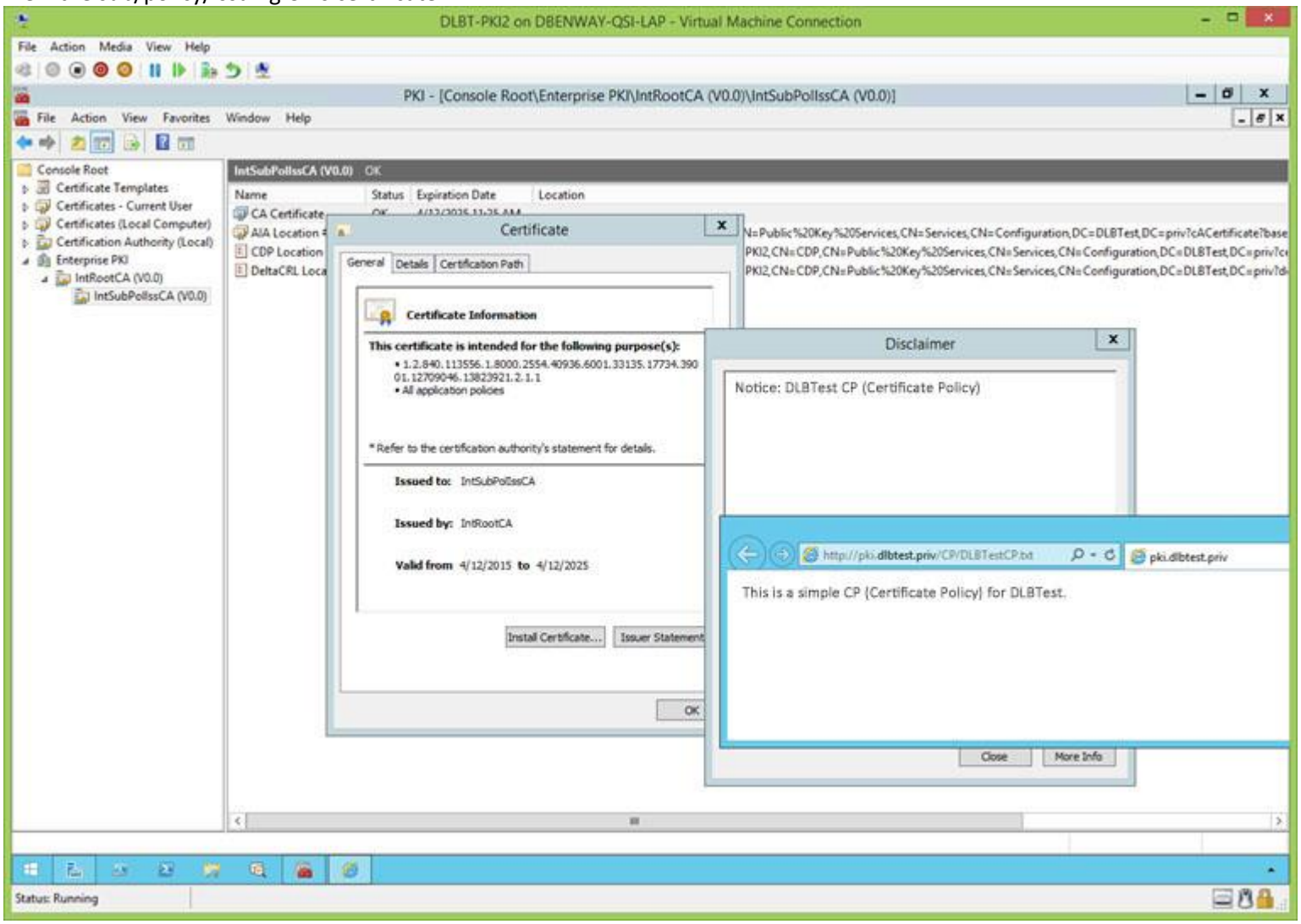
View the sub/policy/issuing CA's Enterprise PKI snap-in, cont'd:



Sub/Policy/Issuing CA's Certificate (Before CertUtil.exe):

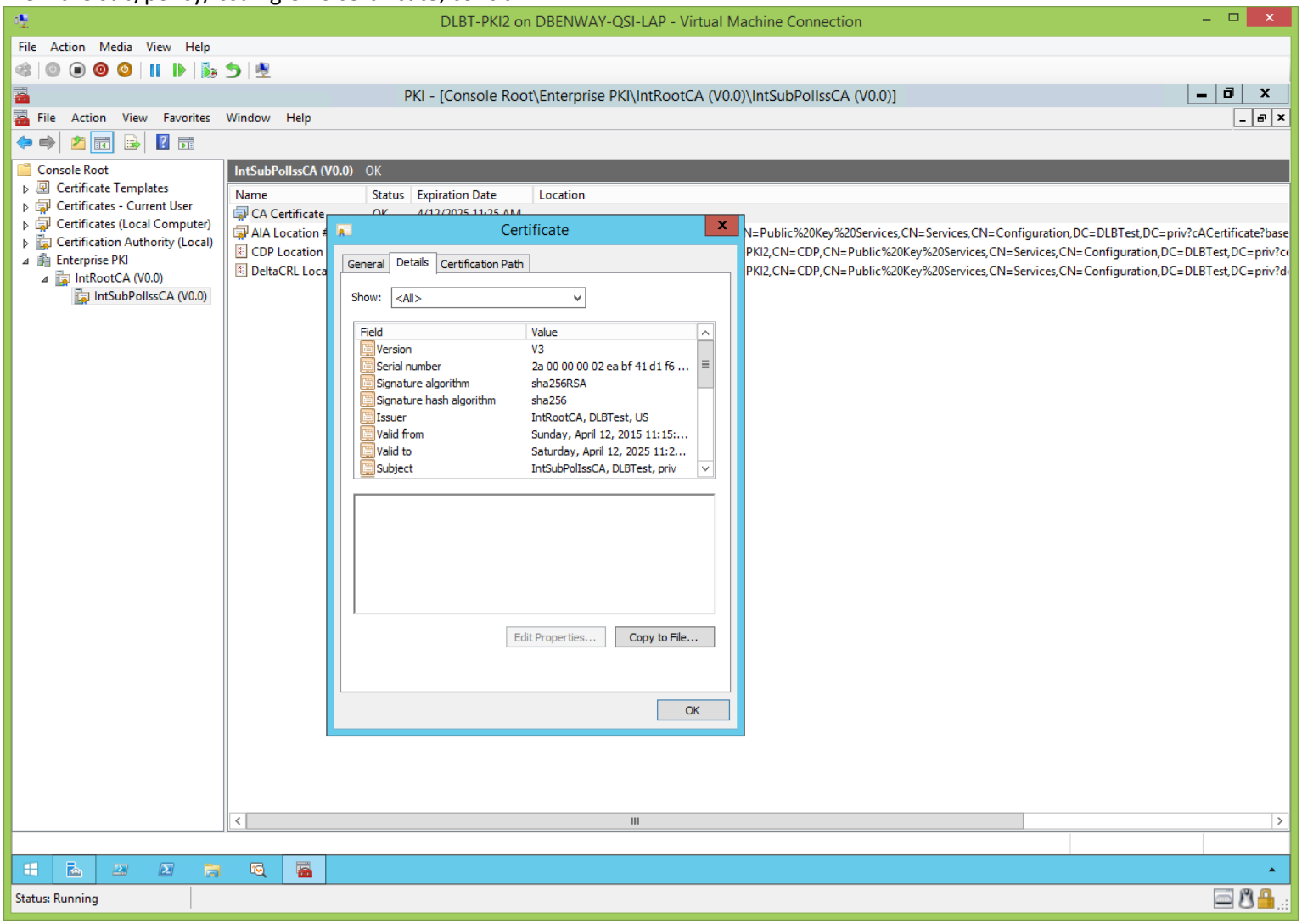
(jump to TOC)

View the sub/policy/issuing CA's certificate:

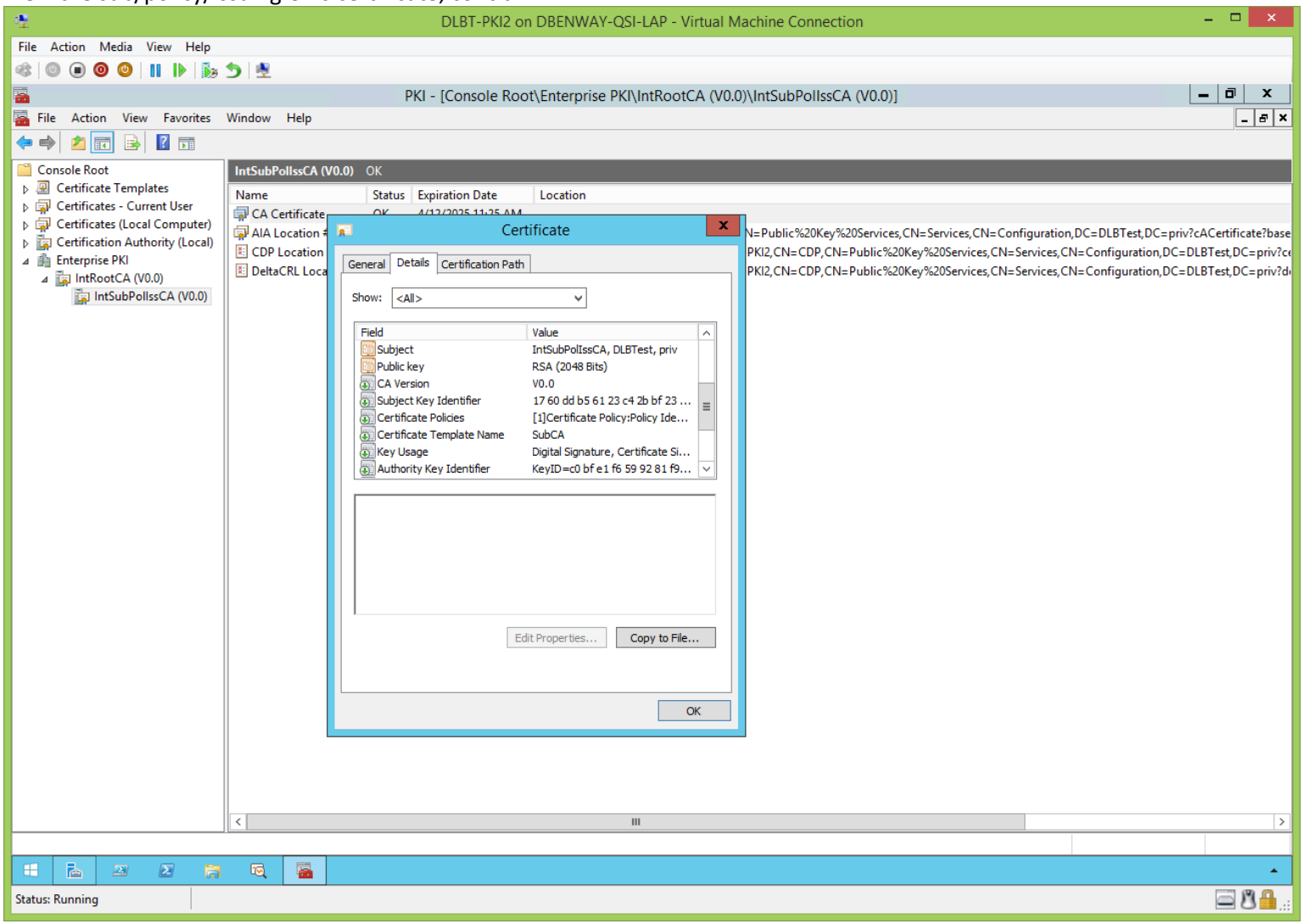


Notice the 'Notice' and 'Issuer Statement' come from the CAPolicy.inf and the CDP respectively.

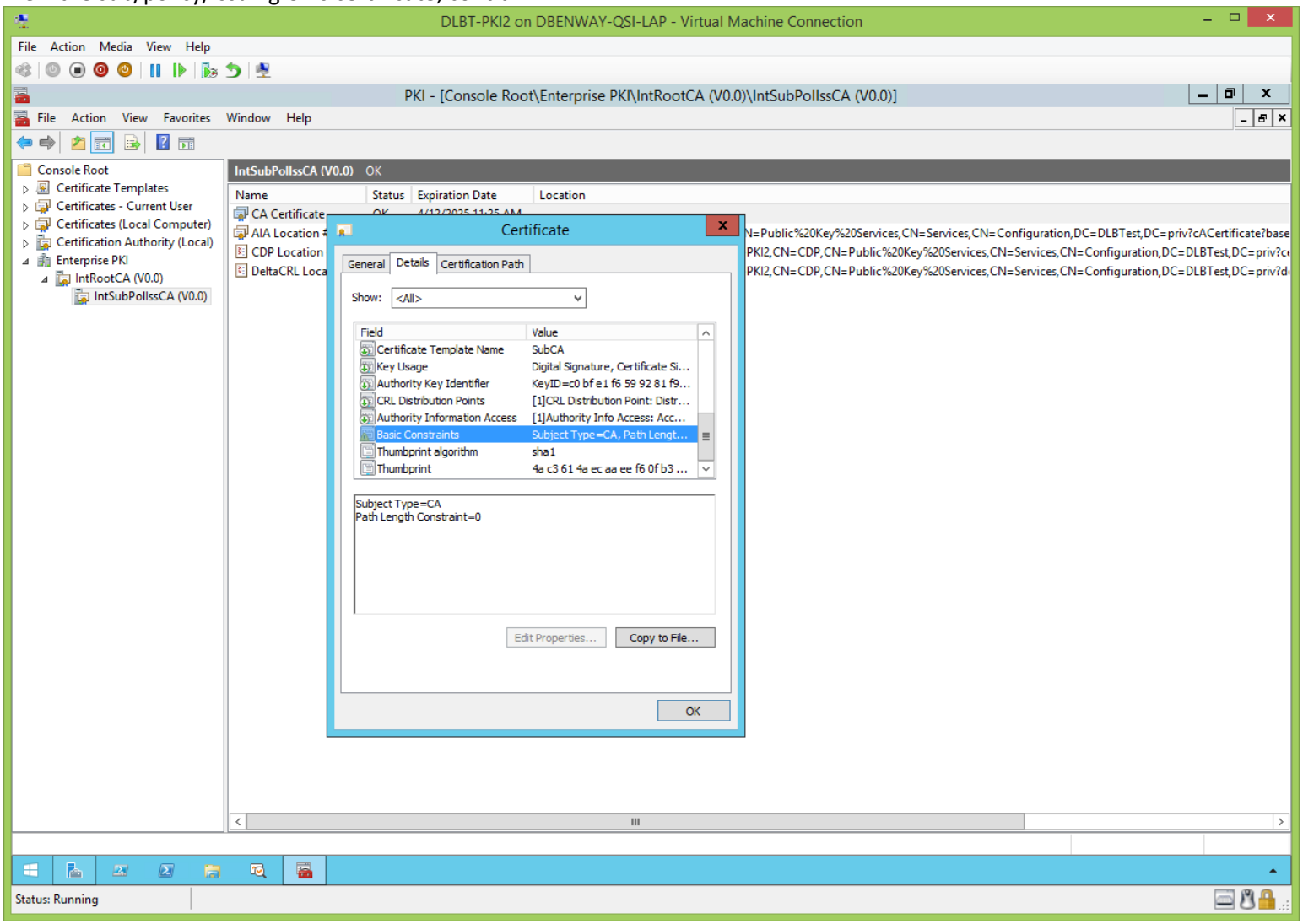
View the sub/policy/issuing CA's certificate, cont'd:



View the sub/policy/issuing CA's certificate, cont'd:

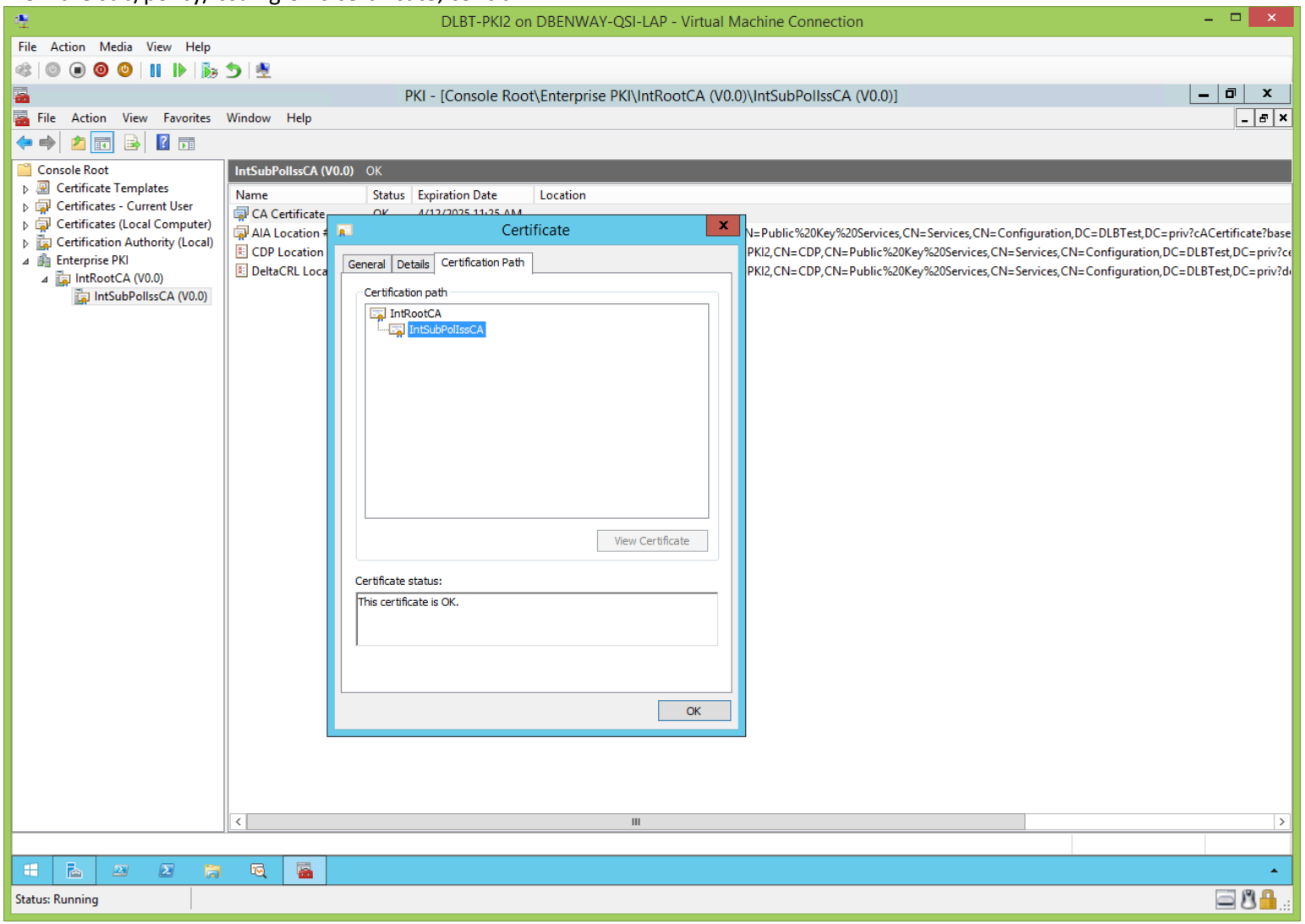


View the sub/policy/issuing CA's certificate, cont'd:



Note: PathLength = 0

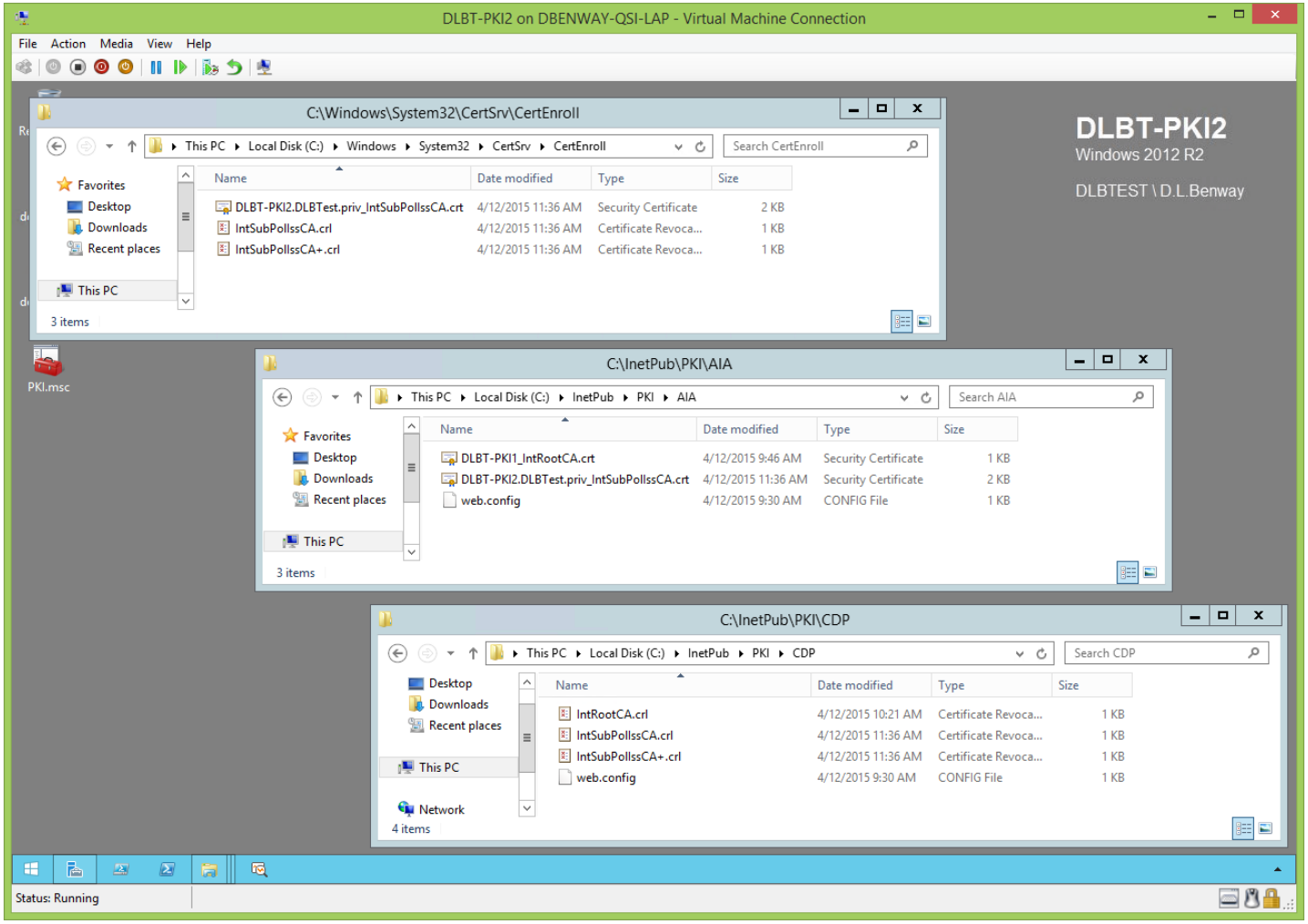
View the sub/policy/issuing CA's certificate, cont'd:



Sub/Policy/Issuing CA Copy Certificate and CRLs to the CDP (Before CertUtil.exe):

(jump to TOC)

Copy the sub/policy/issuing CA's certificate to C:\InetPub\PKI\AIA, copy its CRLs to C:\InetPub\PKI\CDP:



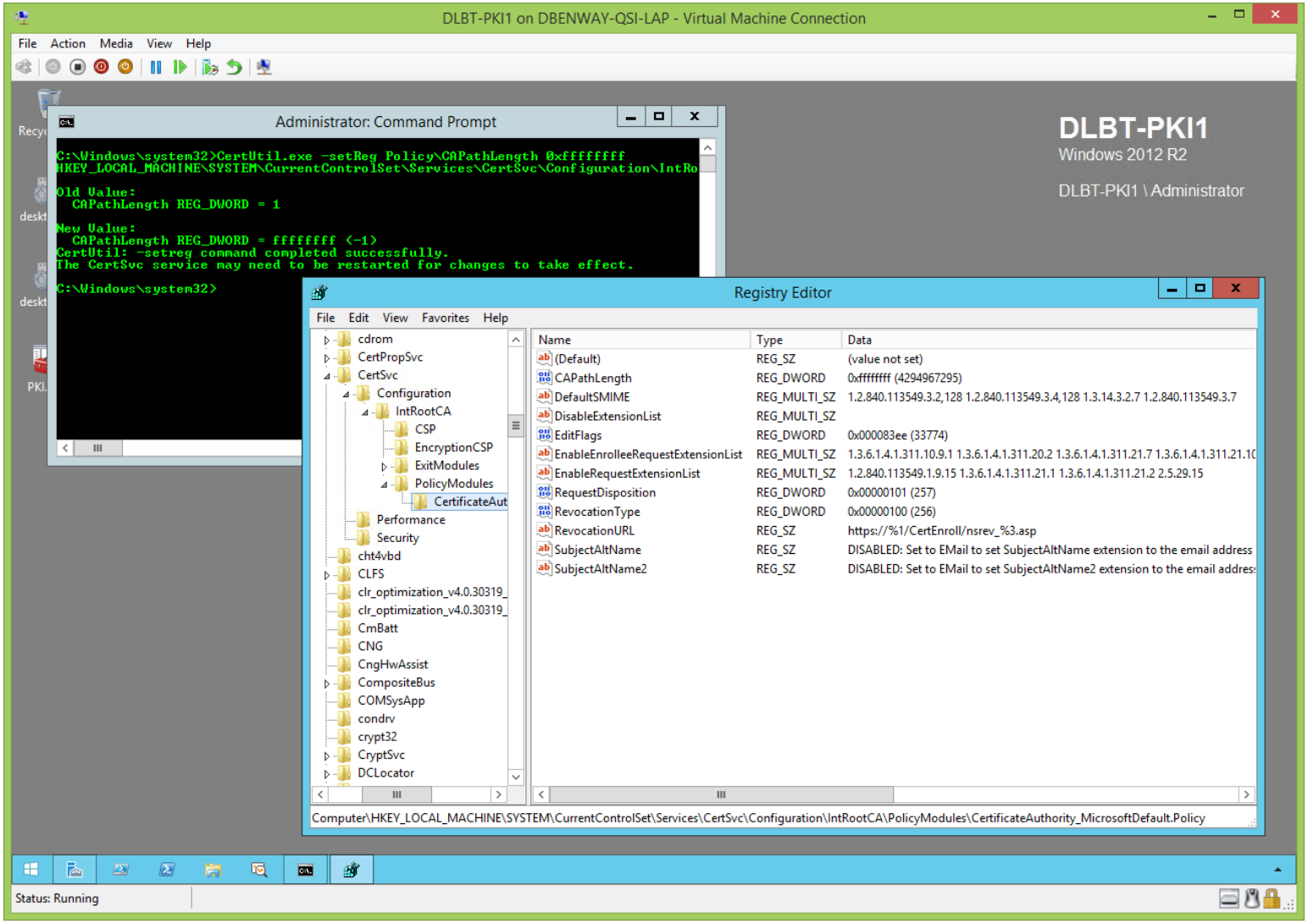
Note: the delta CRL was created before the sub/policy/issuing CA's certUtil.exe reconfigured the sub/policy/issuing CA to no longer create them.

Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's certificate filename contains the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

Sub/Policy/Issuing CA's Path Length Cleanup (Before CertUtil.exe):

(jump to TOC)

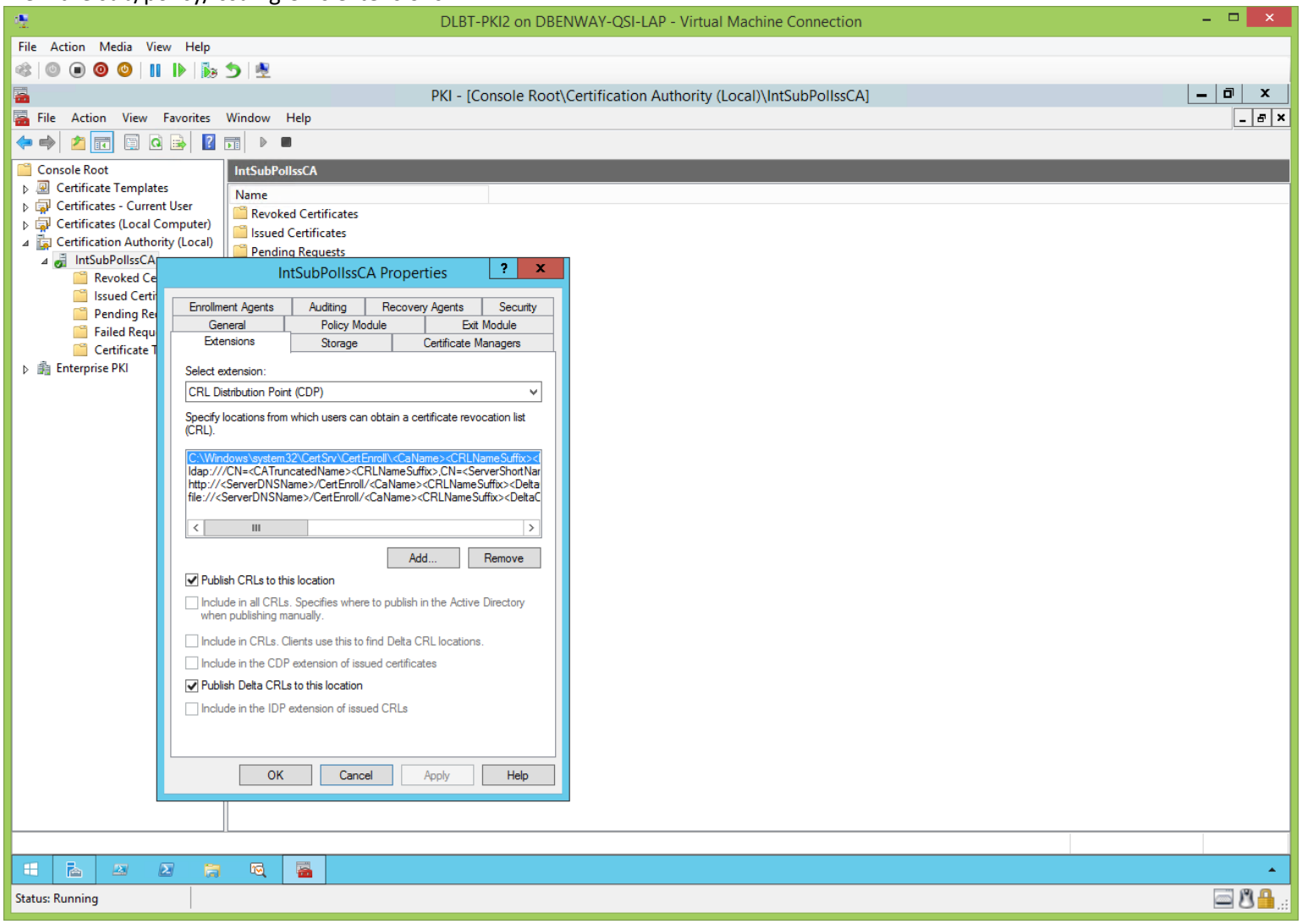
On the root CA, set the Path Length back to 0xffffffff (none), restart ADCS, then shut down the root CA:



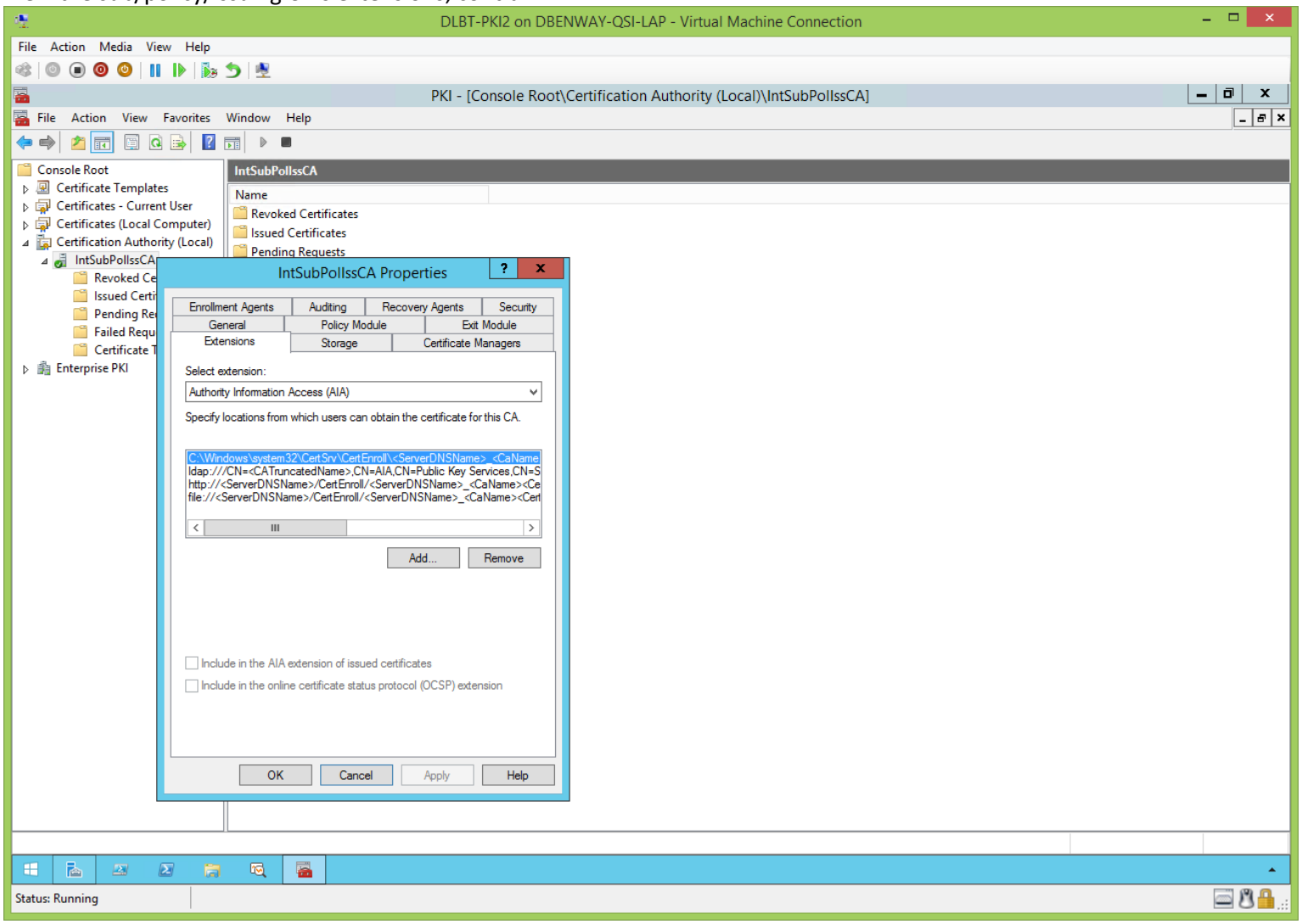
Sub/Policy/Issuing CA's Extensions (Before CertUtil.exe):

(jump to TOC)

View the sub/policy/issuing CA's extensions:



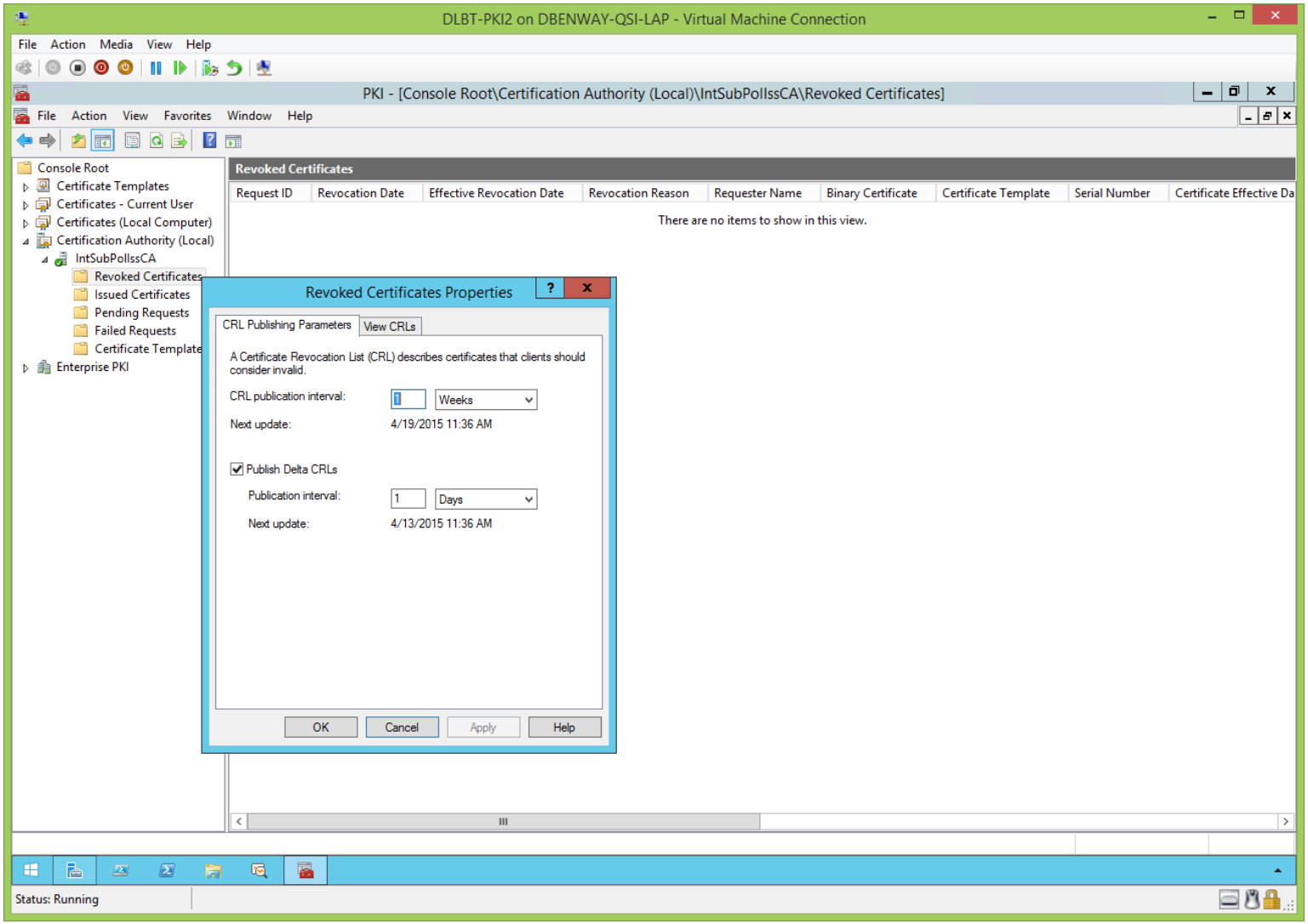
View the sub/policy/issuing CA's extensions, cont'd:



Sub/Policy/Issuing CA's CRLs (Before CertUtil.exe):

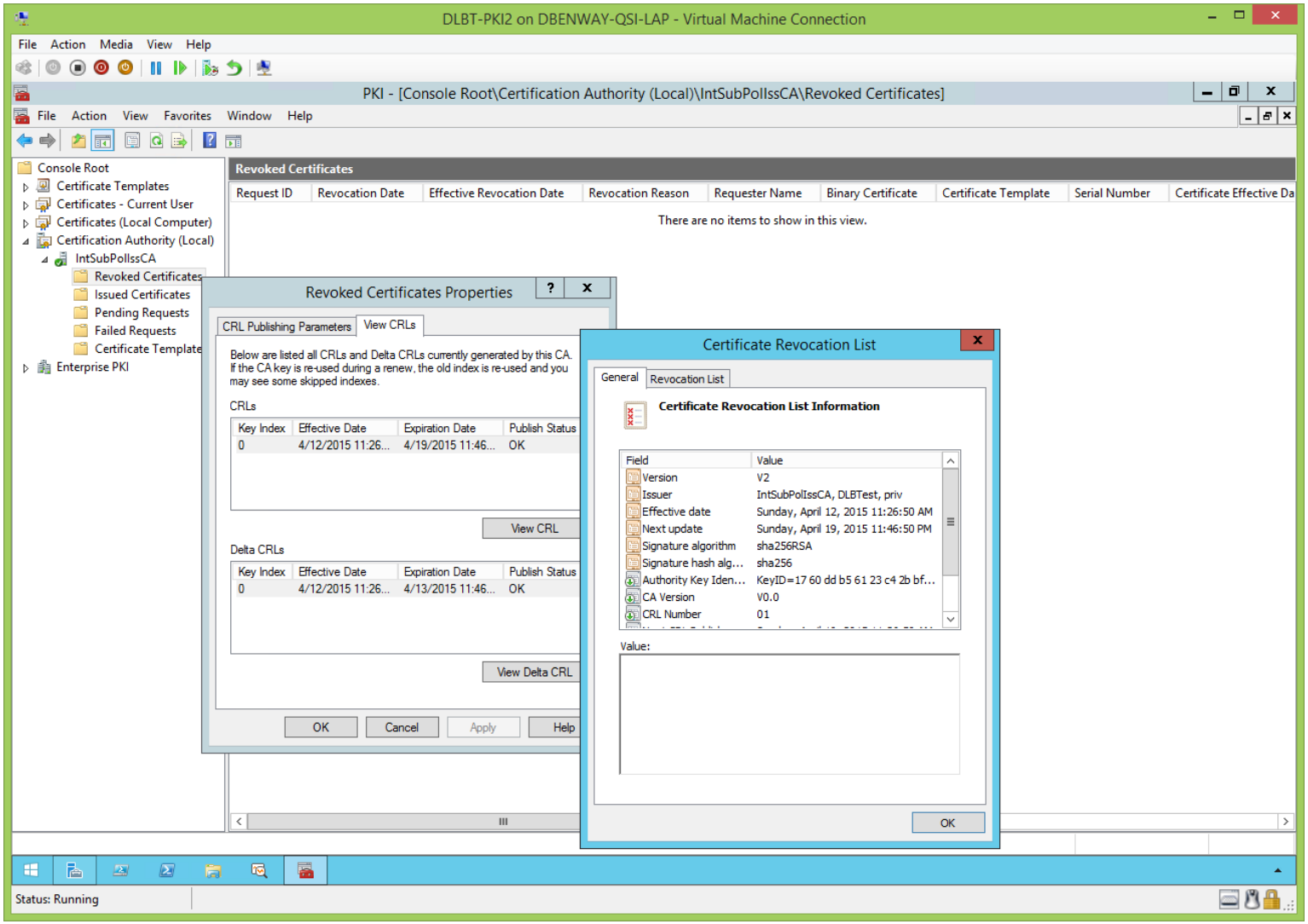
(jump to TOC)

These CRL parameters are properties of the sub/policy/issuing CA, and we'll change these later with CertUtil.exe.

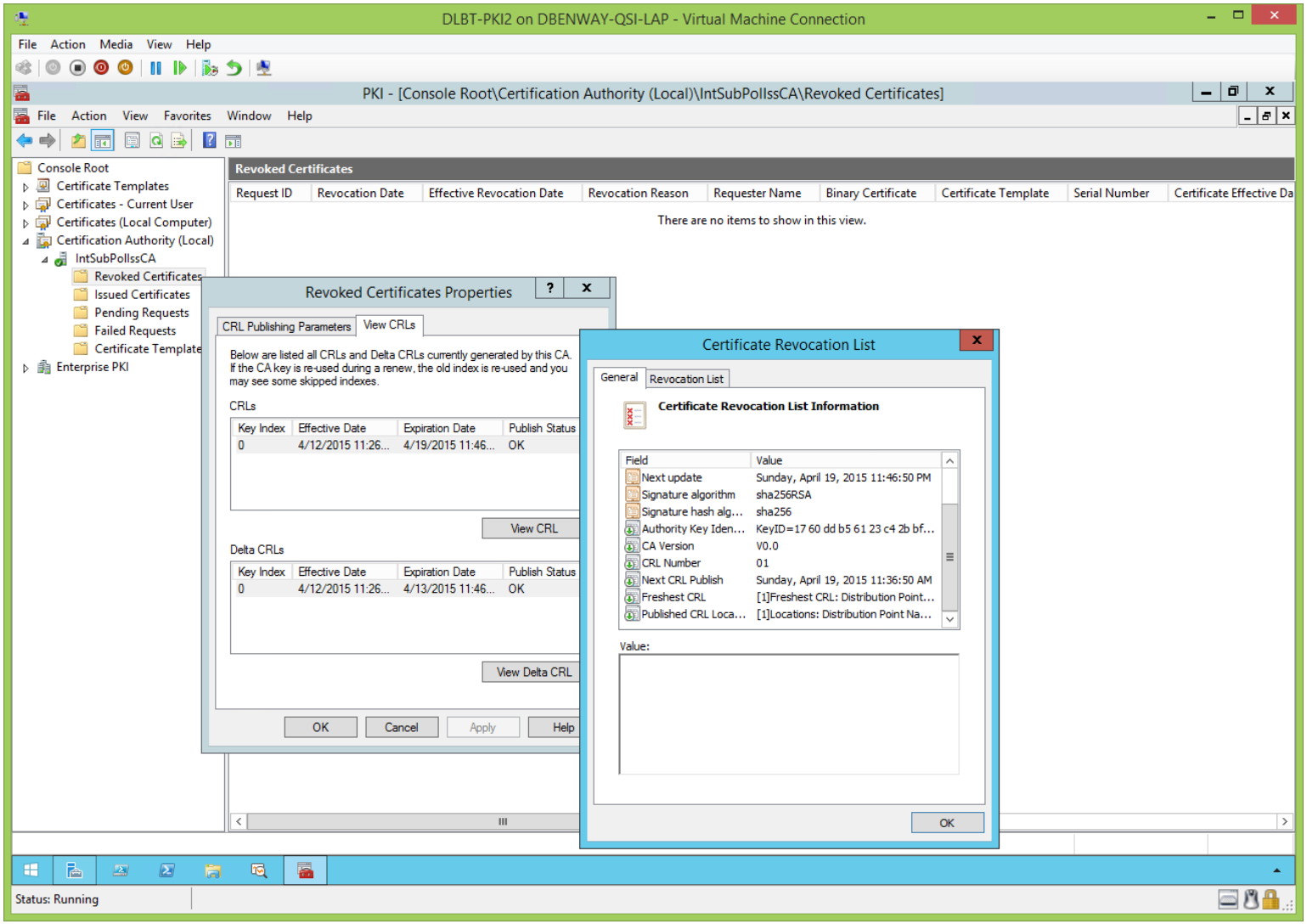


Note: by default, the enterprise sub/policy/issuing CA does publish delta CRLs (this was not set in the sub/policy/issuing CA's CAPolicy.inf, and we have not yet run the certUtil.exe commands).

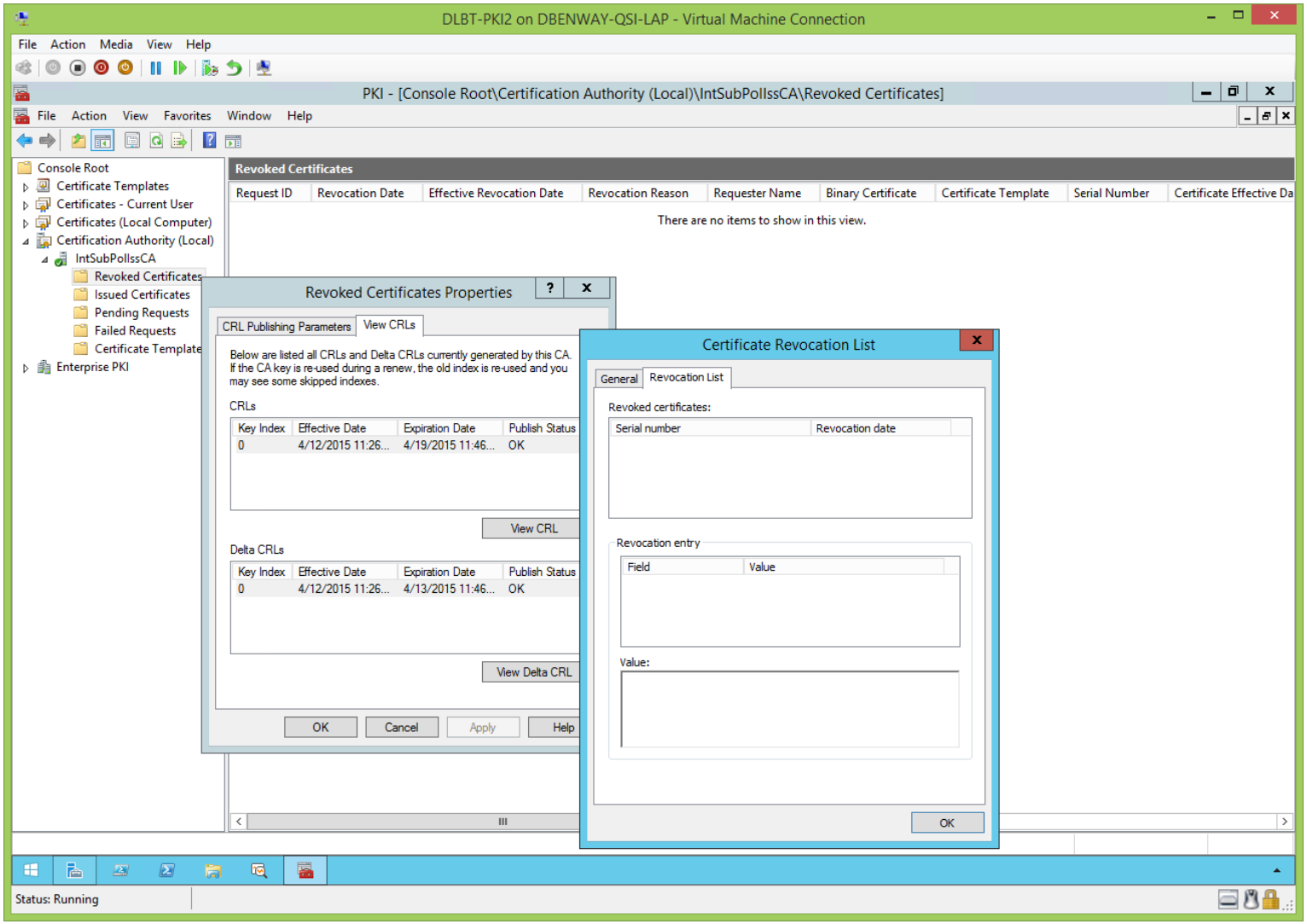
View the sub/policy/issuing CA's CRL properties, cont'd:



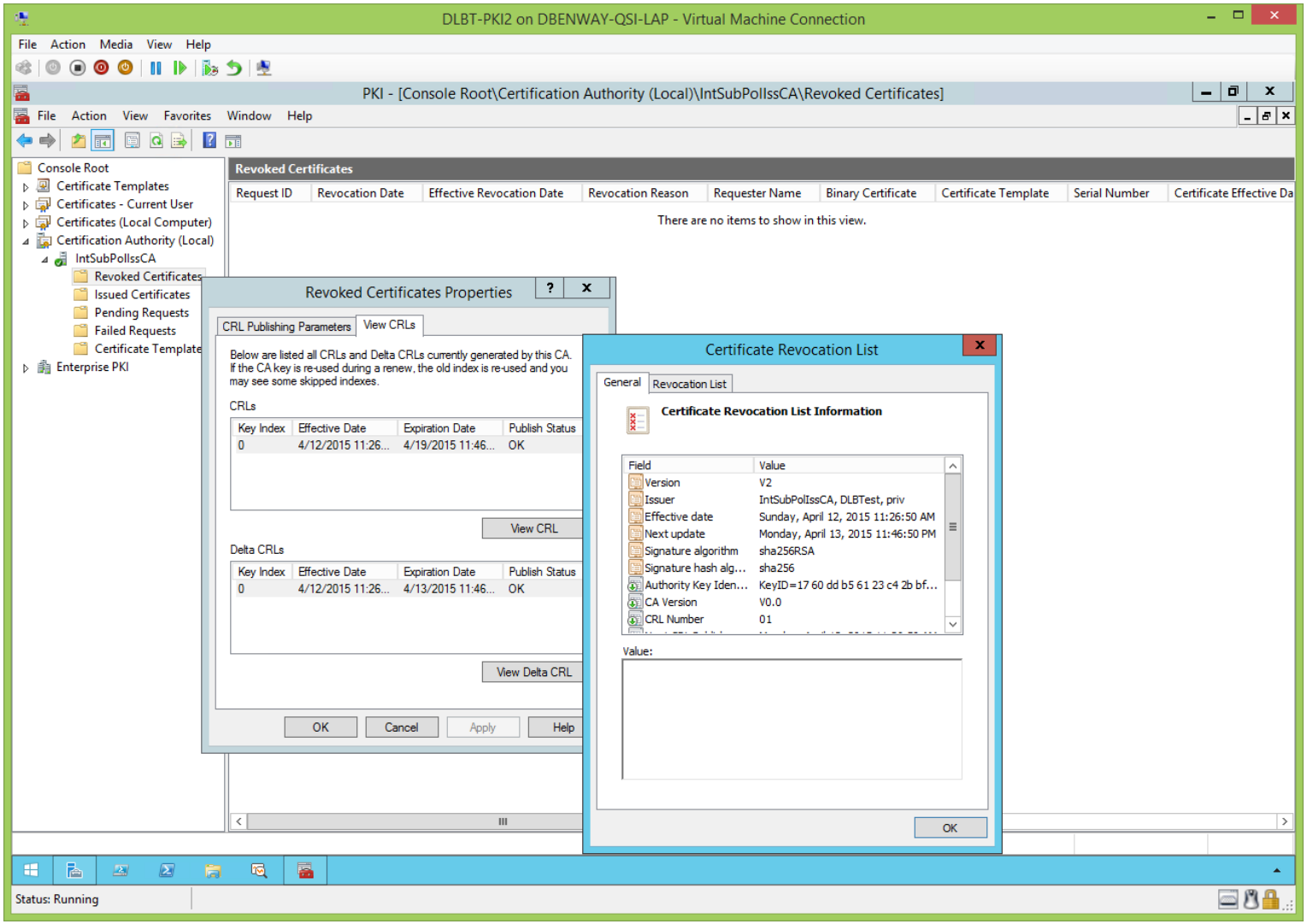
View the sub/policy/issuing CA's CRL properties, cont'd:



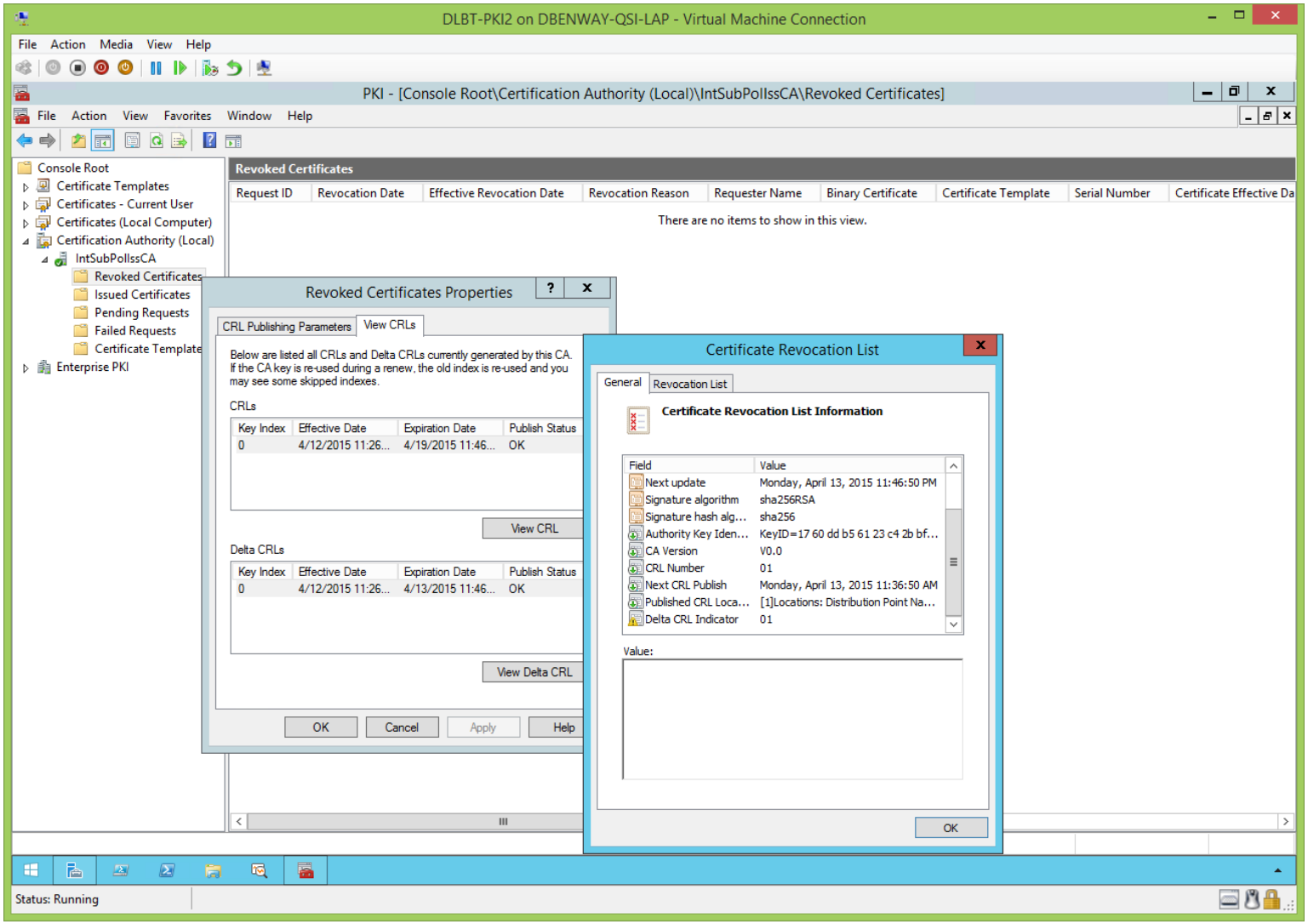
View the sub/policy/issuing CA's CRL properties, cont'd:



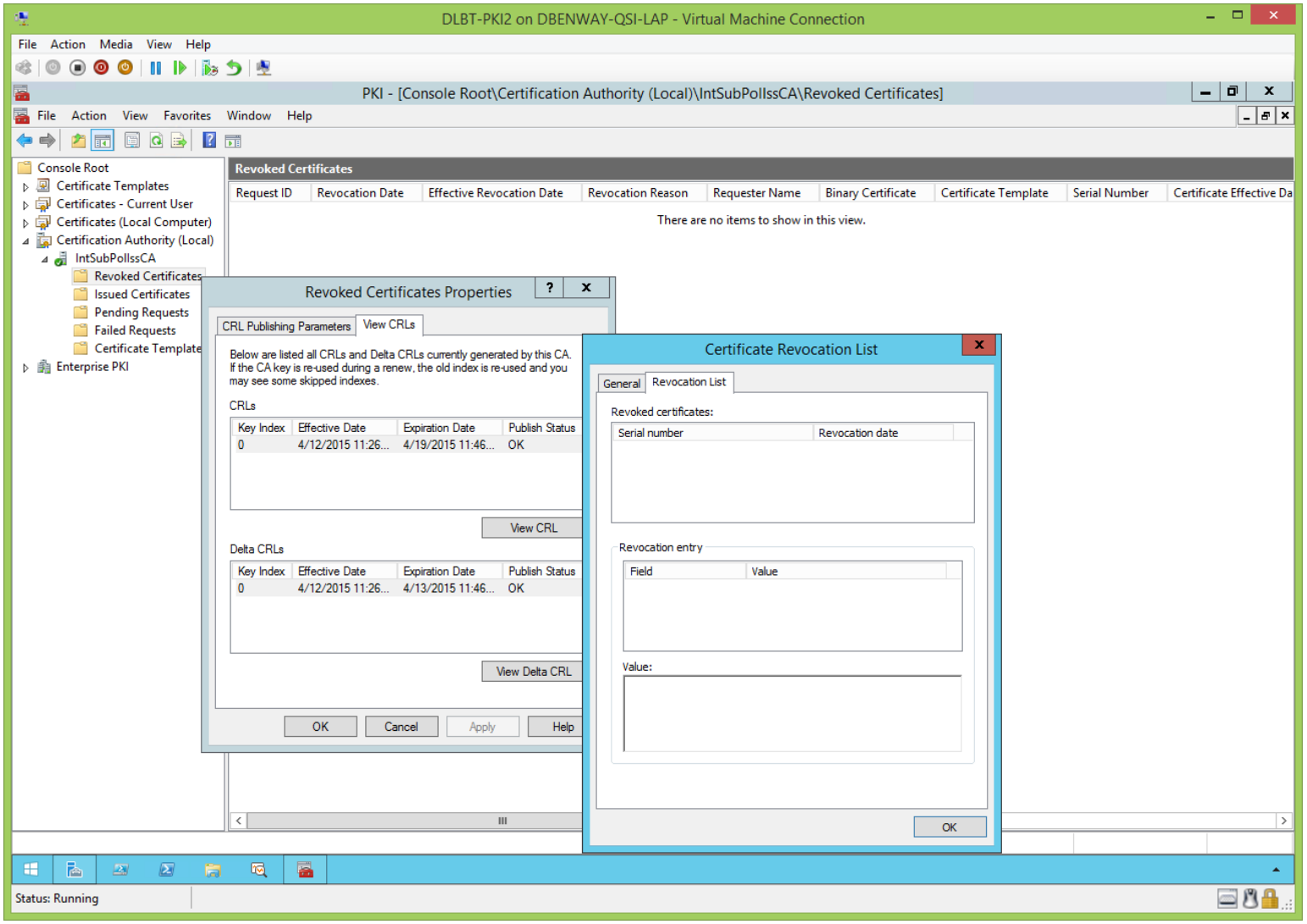
View the sub/policy/issuing CA's CRL properties, cont'd:



View the sub/policy/issuing CA's CRL properties, cont'd:



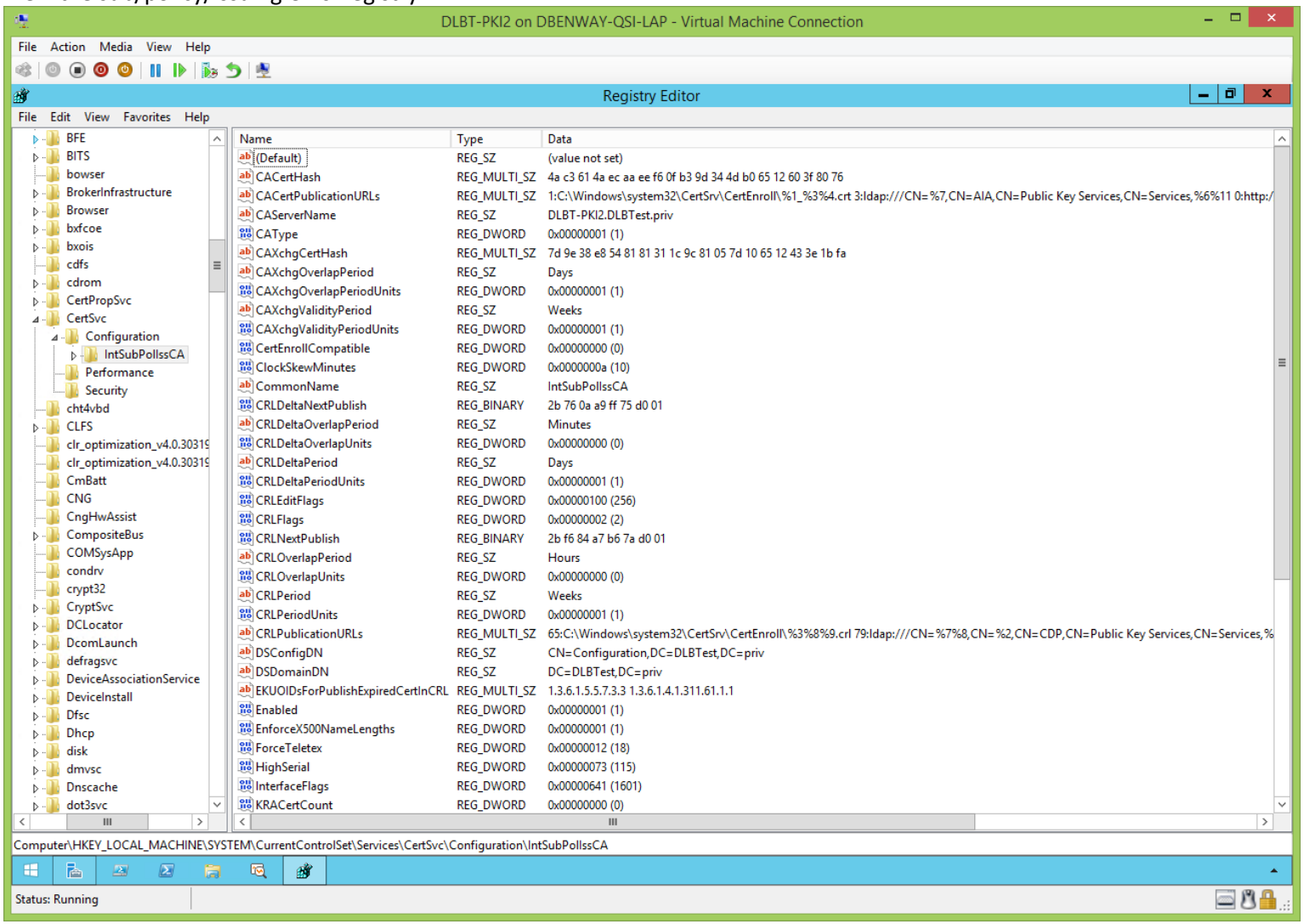
View the sub/policy/issuing CA's CRL properties, cont'd:



Sub/Policy/Issuing CA's Registry (Before CertUtil.exe):

(jump to TOC)

View the sub/policy/issuing CA's Registry:



View the sub/policy/issuing CA's Registry, cont'd:

DLBT-PKI2 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

Registry Editor

File Edit View Favorites Help

BFE
BITS
bowser
BrokerInfrastructure
Browser
bxfcoe
bxois
cdfs
cdrom
CertPropSvc
CertSvc
Configuration
IntSubPolIssCA
Performance
Security
cht4vbd
CLFS
clr_optimization_v4.0.30319
clr_optimization_v4.0.30319
CmBatt
CNG
CngHwAssist
CompositeBus
COMSysApp
condrv
crypt32
CryptSvc
DCLocator
DcomLaunch
defragsvc
DeviceAssociationService
DeviceInstall
Dfsc
Dhcp
disk
dmvsc
Dnscache
dot3svc

Name	Type	Data
CRLDeltaPeriodUnits	REG_DWORD	0x00000001 (1)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	2b f6 84 a7 b6 7a d0 01
CRLOverlapPeriod	REG_SZ	Hours
CRLOverlapUnits	REG_DWORD	0x00000000 (0)
CRLPeriod	REG_SZ	Weeks
CRLPeriodUnits	REG_DWORD	0x00000001 (1)
CRLPublicationURLs	REG_MULTI_SZ	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl 79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%
DSConfigDN	REG_SZ	CN=Configuration,DC=DLBTest,DC=priv
DSDomainDN	REG_SZ	DC=DLBTest,DC=priv
EKUOIDsForPublishExpiredCertInCRL	REG_MULTI_SZ	1.3.6.1.5.5.7.3.3 1.3.6.1.4.1.311.61.1.1
Enabled	REG_DWORD	0x00000001 (1)
EnforceX500NameLengths	REG_DWORD	0x00000001 (1)
ForceTeletex	REG_DWORD	0x00000012 (18)
HighSerial	REG_DWORD	0x00000073 (115)
InterfaceFlags	REG_DWORD	0x00000641 (1601)
KRACertCount	REG_DWORD	0x00000000 (0)
KRACertHash	REG_MULTI_SZ	
KRAFlags	REG_DWORD	0x00000000 (0)
LogLevel	REG_DWORD	0x00000003 (3)
MaxIncomingAllocSize	REG_DWORD	0x00010000 (65536)
MaxIncomingMessageSize	REG_DWORD	0x00010000 (65536)
PolicyFlags	REG_DWORD	0x00000000 (0)
RequestFileName	REG_SZ	C:\DLBT-PKI2.DLBTest.priv_DLBTest-DLBT-PKI2-CA%4.req
Security	REG_BINARY	01 00 14 84 20 01 00 00 30 01 00 00 14 00 00 00 44 00 00 00 02 00 30 00 02 00 00 00 02 c0 14 00 ff ff 00 00 01 01 00 00 00 00 00 01 00 00 00 00 02
SetupStatus	REG_DWORD	0x00000001 (1)
SignedAttributes	REG_MULTI_SZ	RequesterName
SubjectTemplate	REG_MULTI_SZ	EMail CommonName OrganizationalUnit Organization Locality State DomainComponent Country
UseDS	REG_DWORD	0x00000001 (1)
ValidityPeriod	REG_SZ	Years
ValidityPeriodUnits	REG_DWORD	0x00000002 (2)
ViewAgeMinutes	REG_DWORD	0x00000010 (16)
ViewIdleMinutes	REG_DWORD	0x00000008 (8)

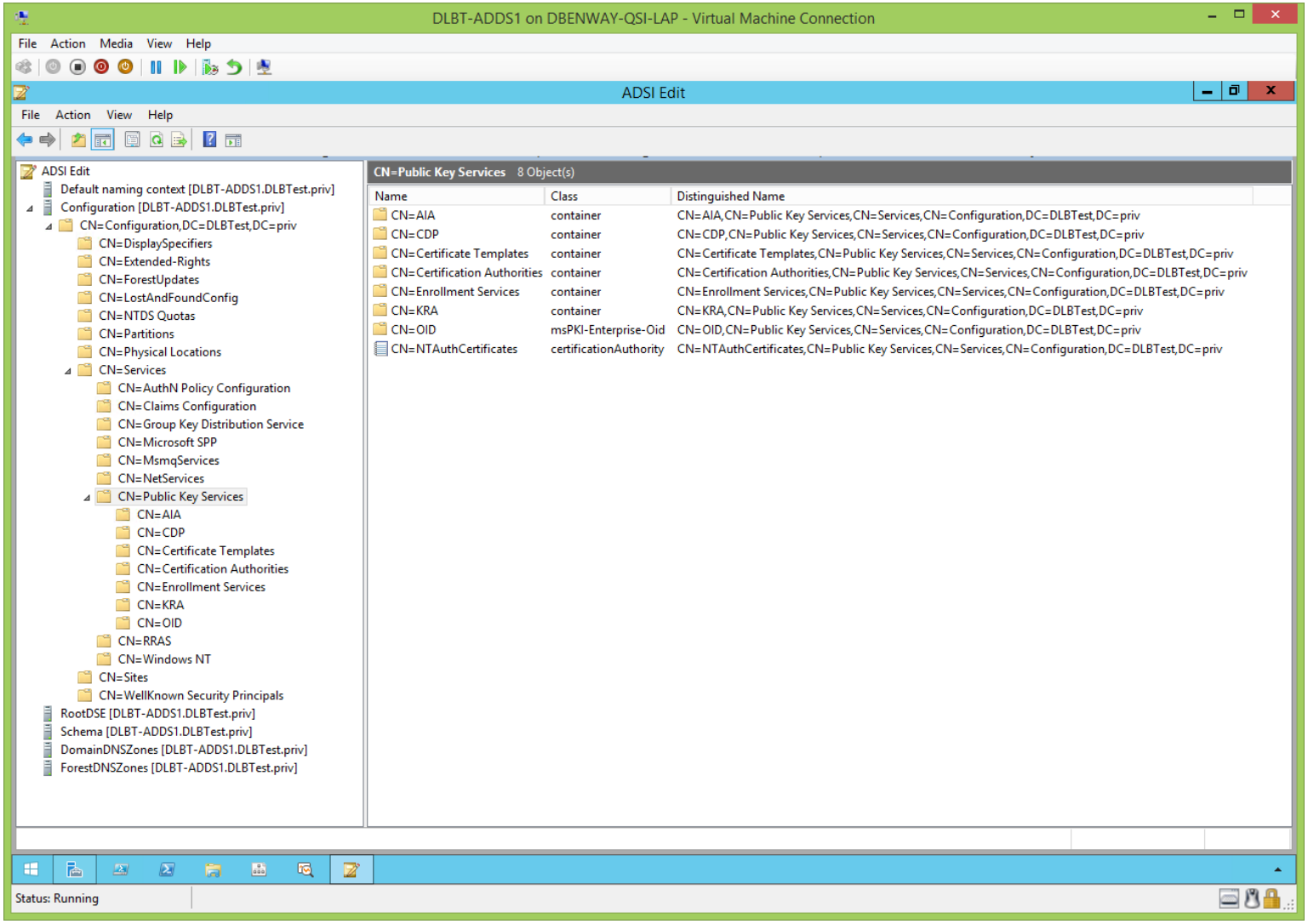
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\IntSubPolIssCA

Status: Running

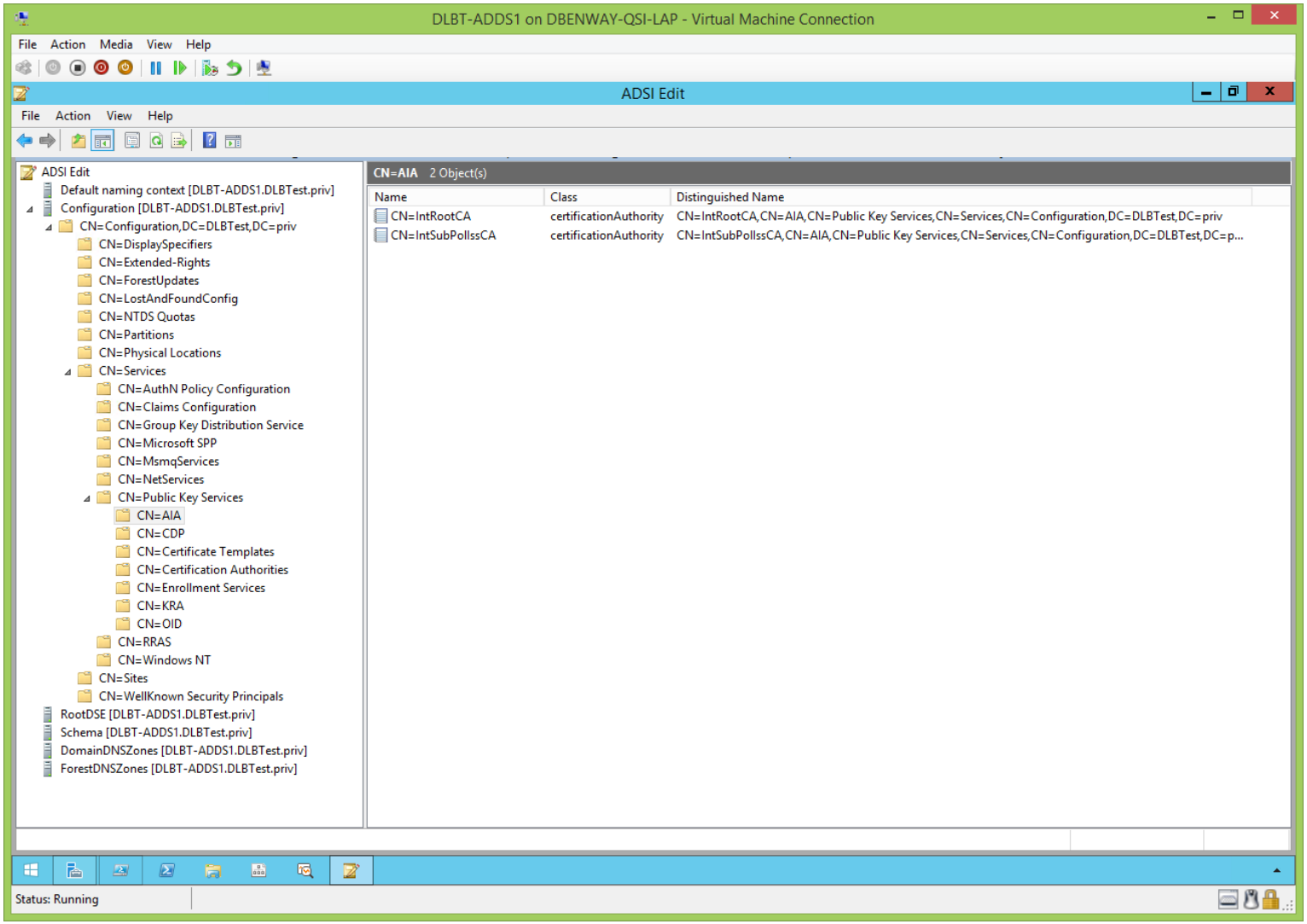
ADSIEdit.msc (Before CertUtil.exe):

(jump to TOC)

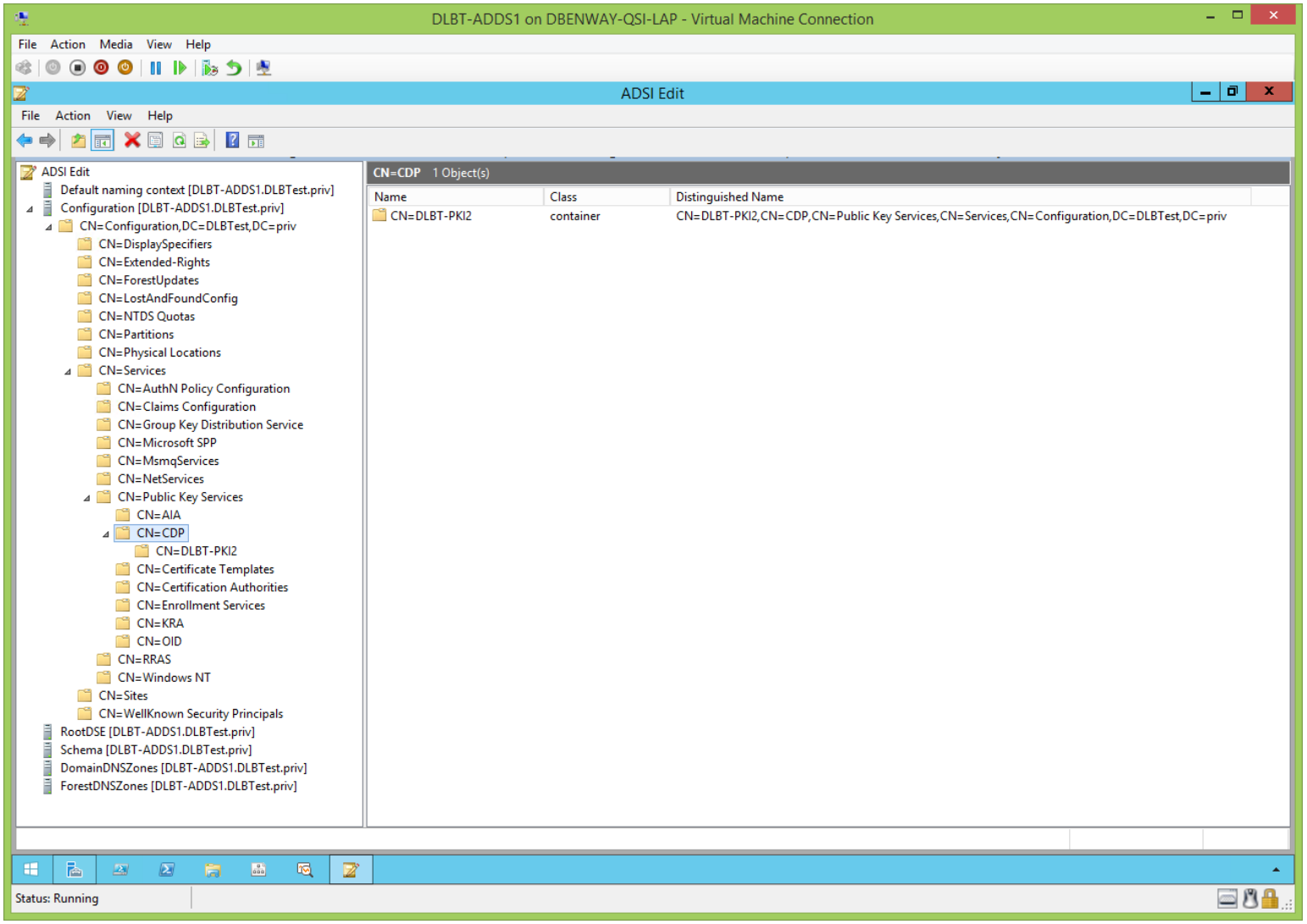
View ADSIEdit.msc:



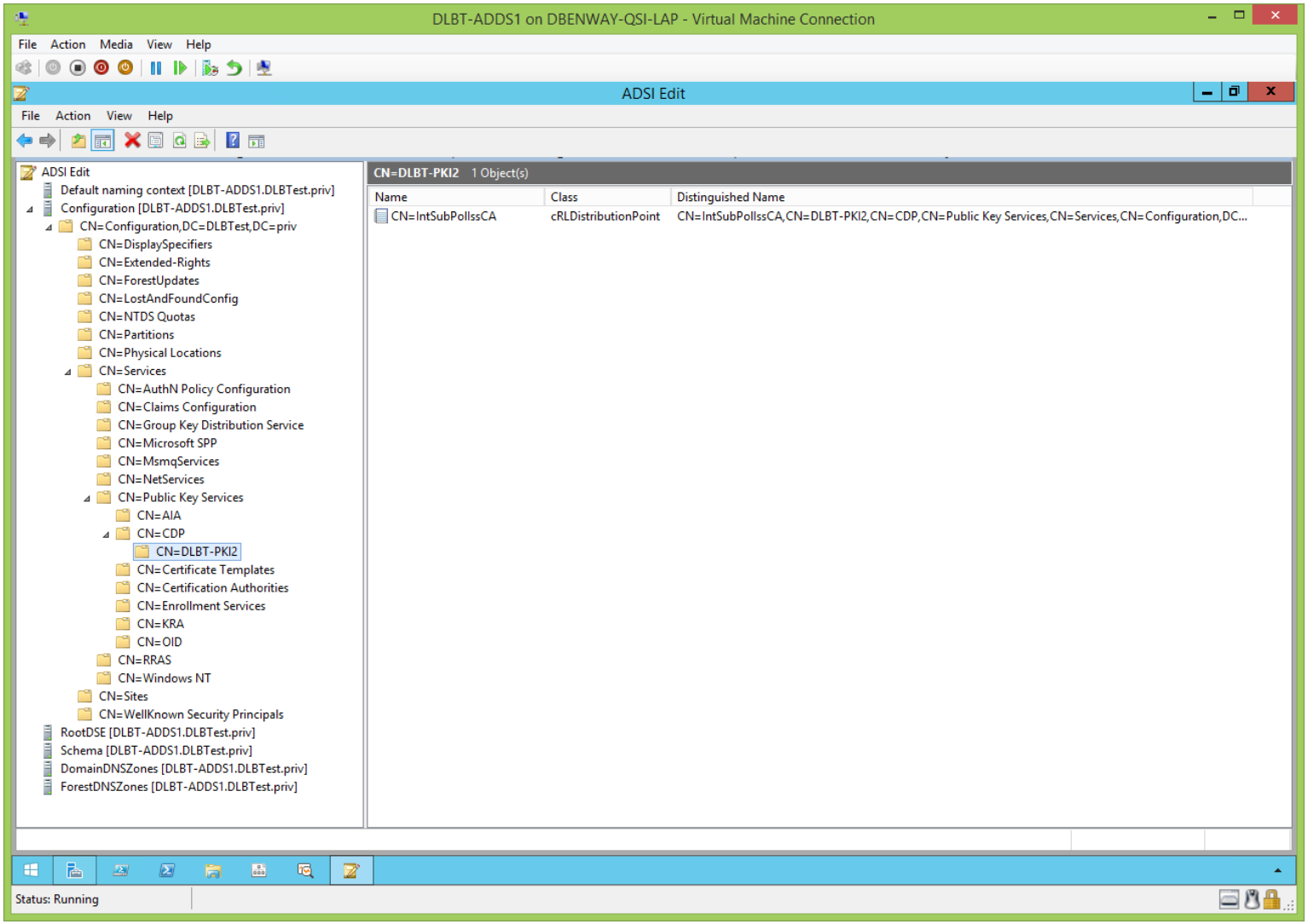
View ADSIEdit.msc, cont'd:



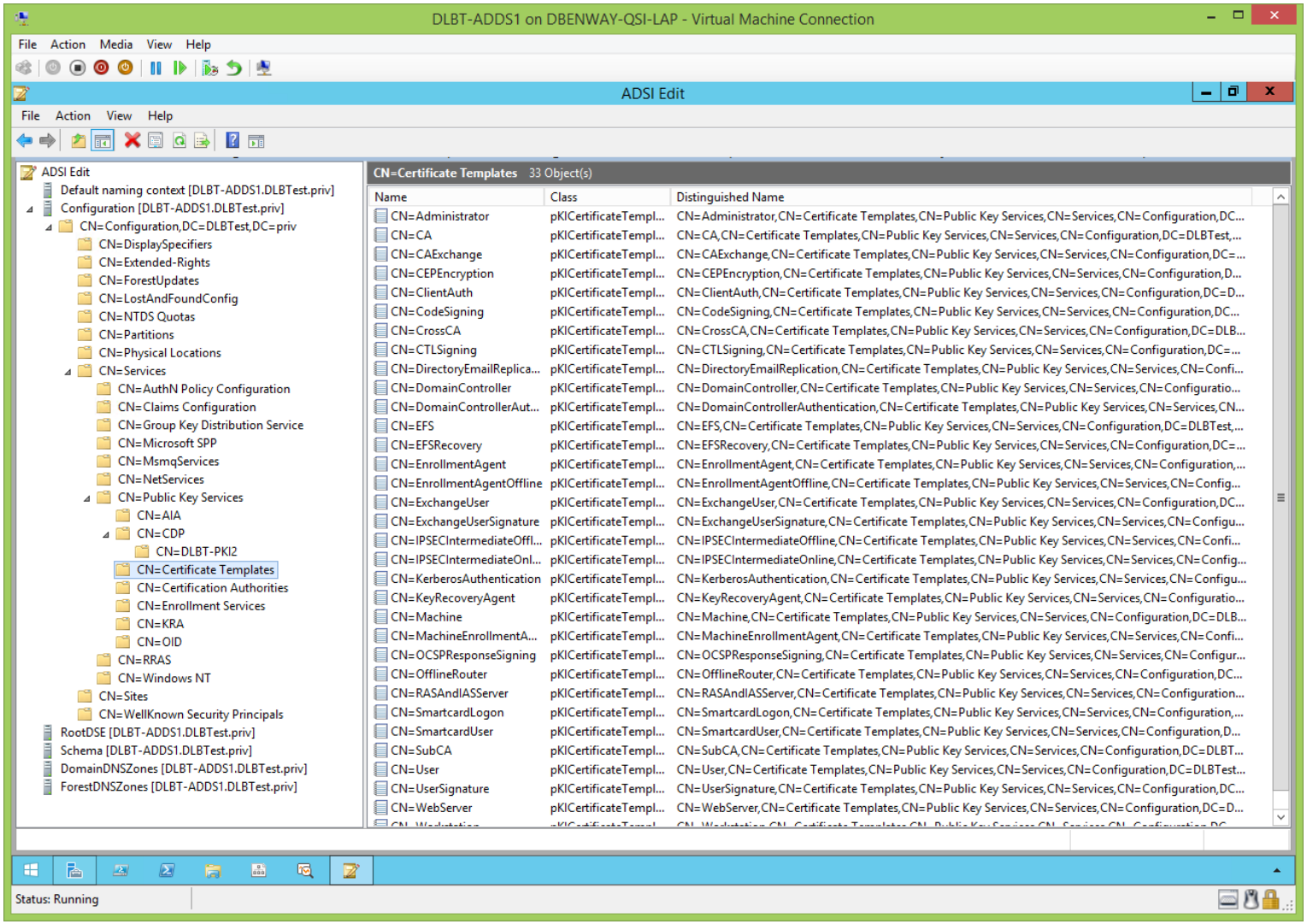
View ADSIEdit.msc, cont'd:



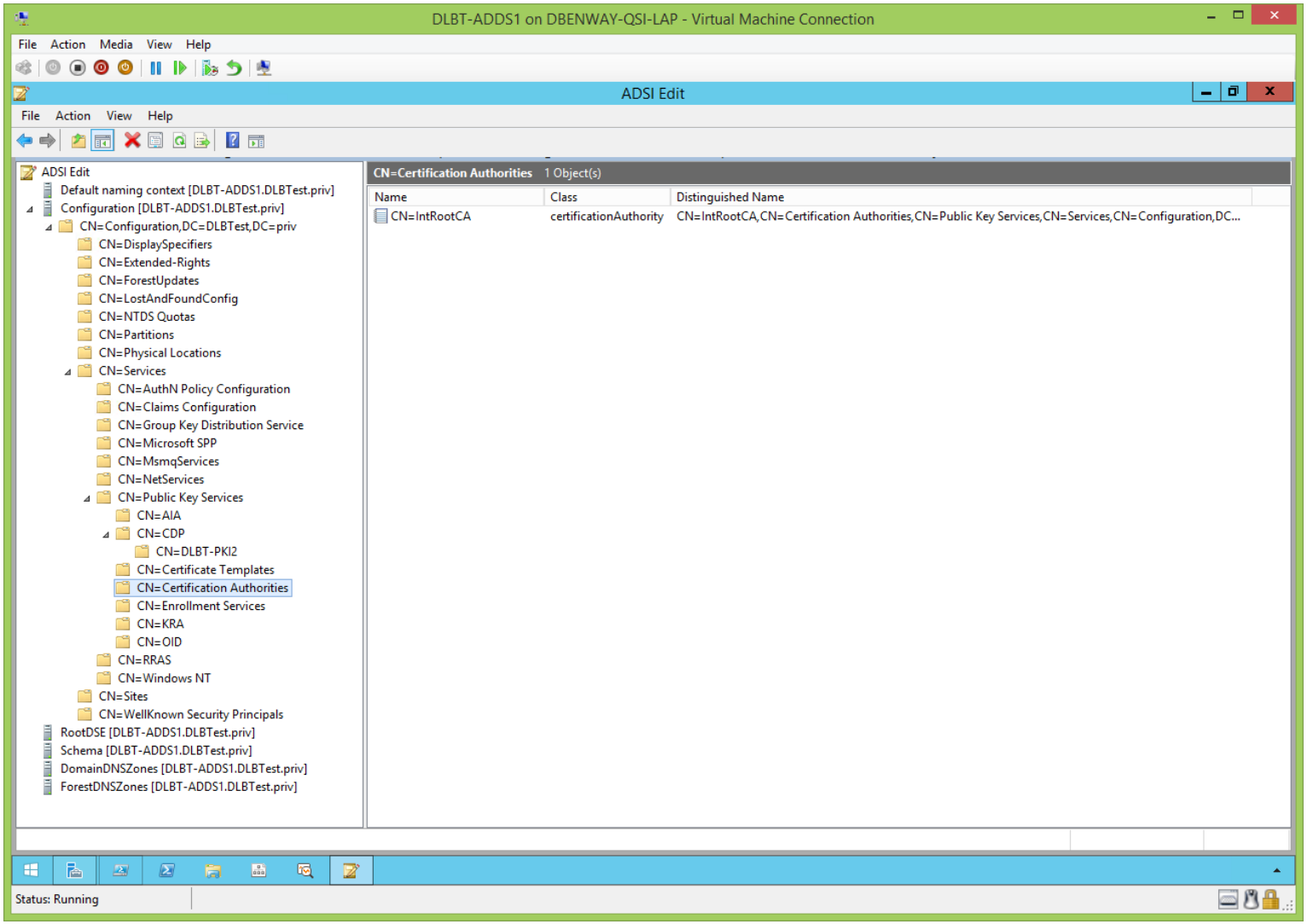
View ADSIEdit.msc, cont'd:



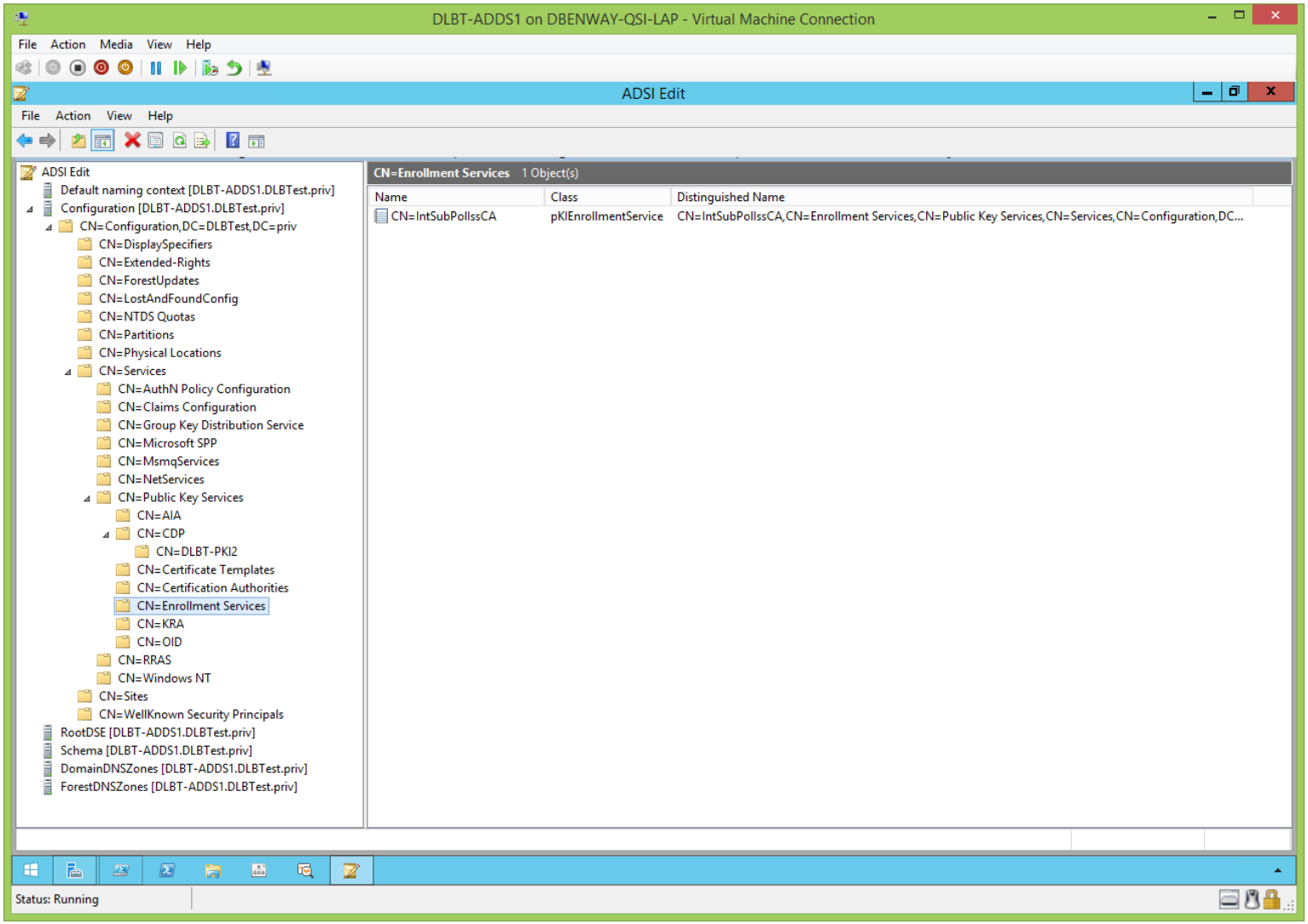
View ADSIEdit.msc, cont'd:



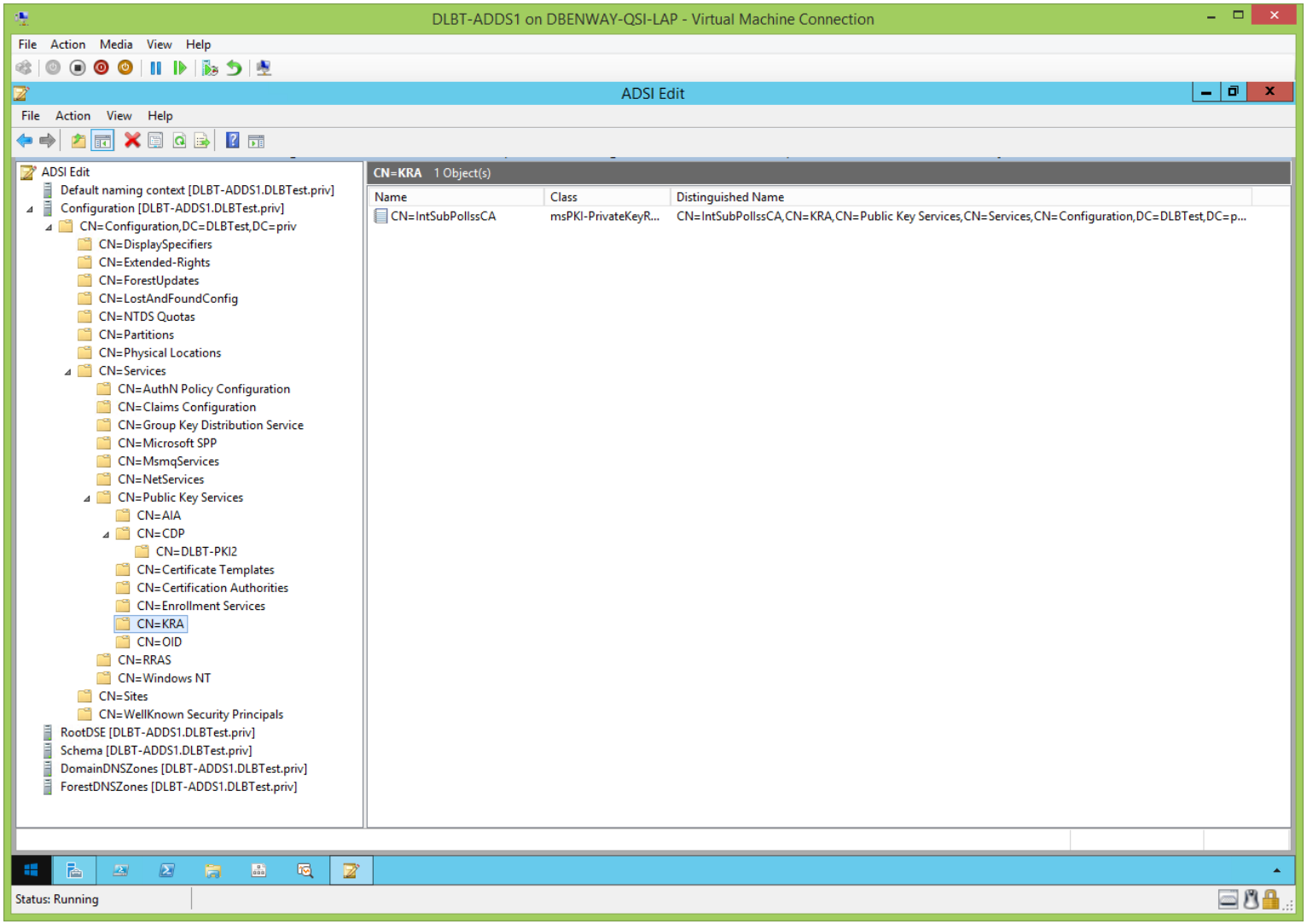
View ADSIEdit.msc, cont'd:



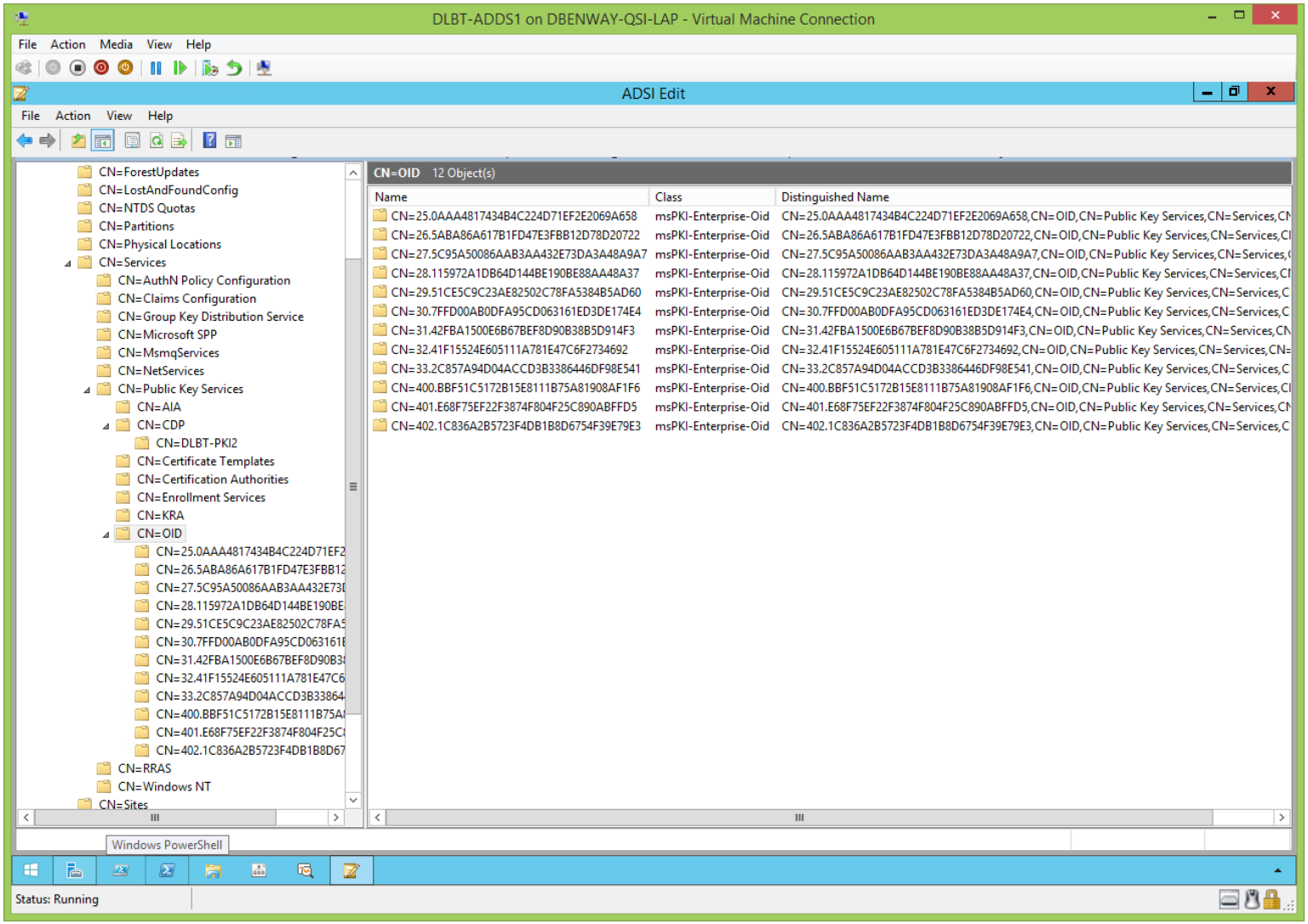
View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:



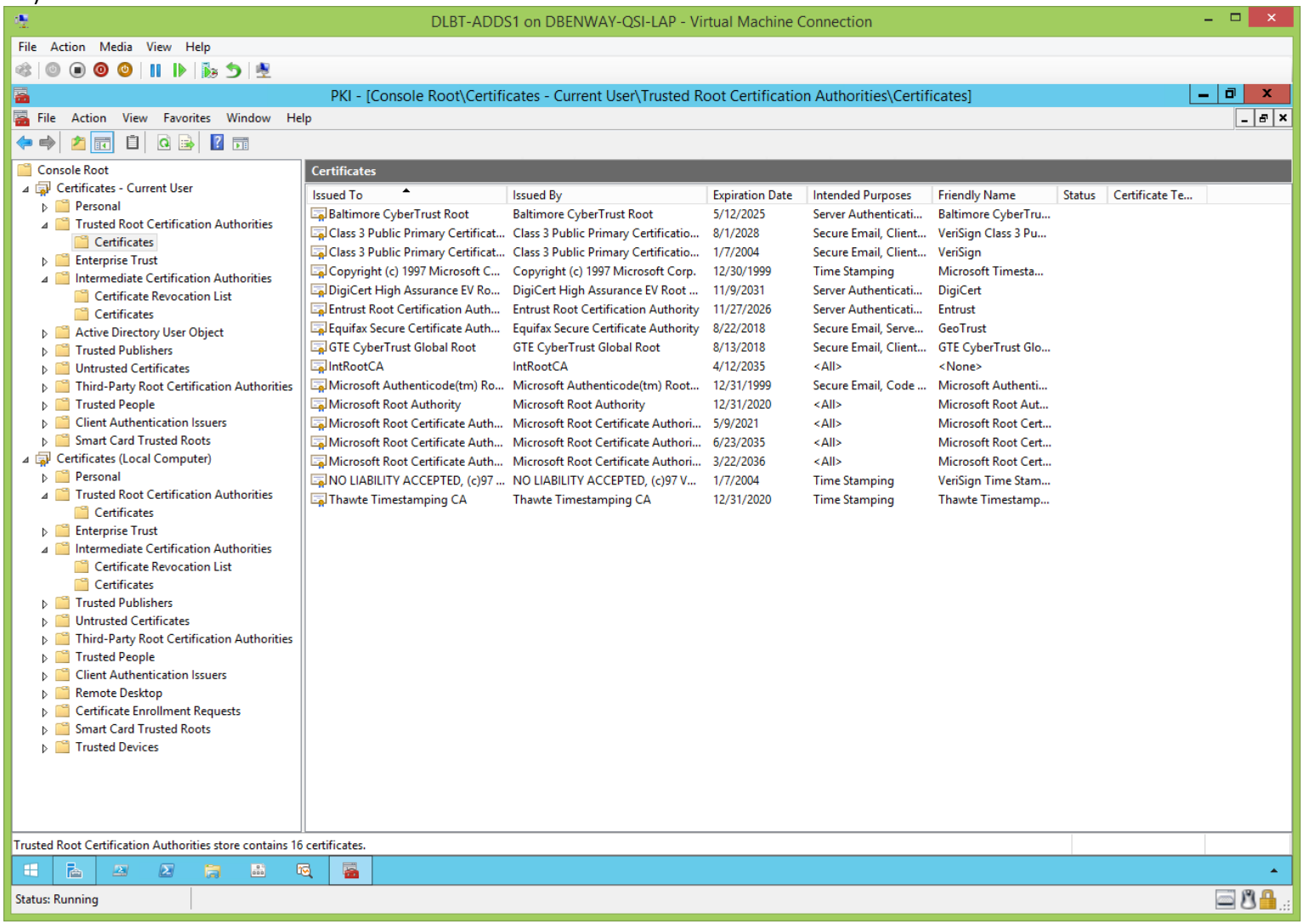
View ADSIEdit.msc, cont'd:



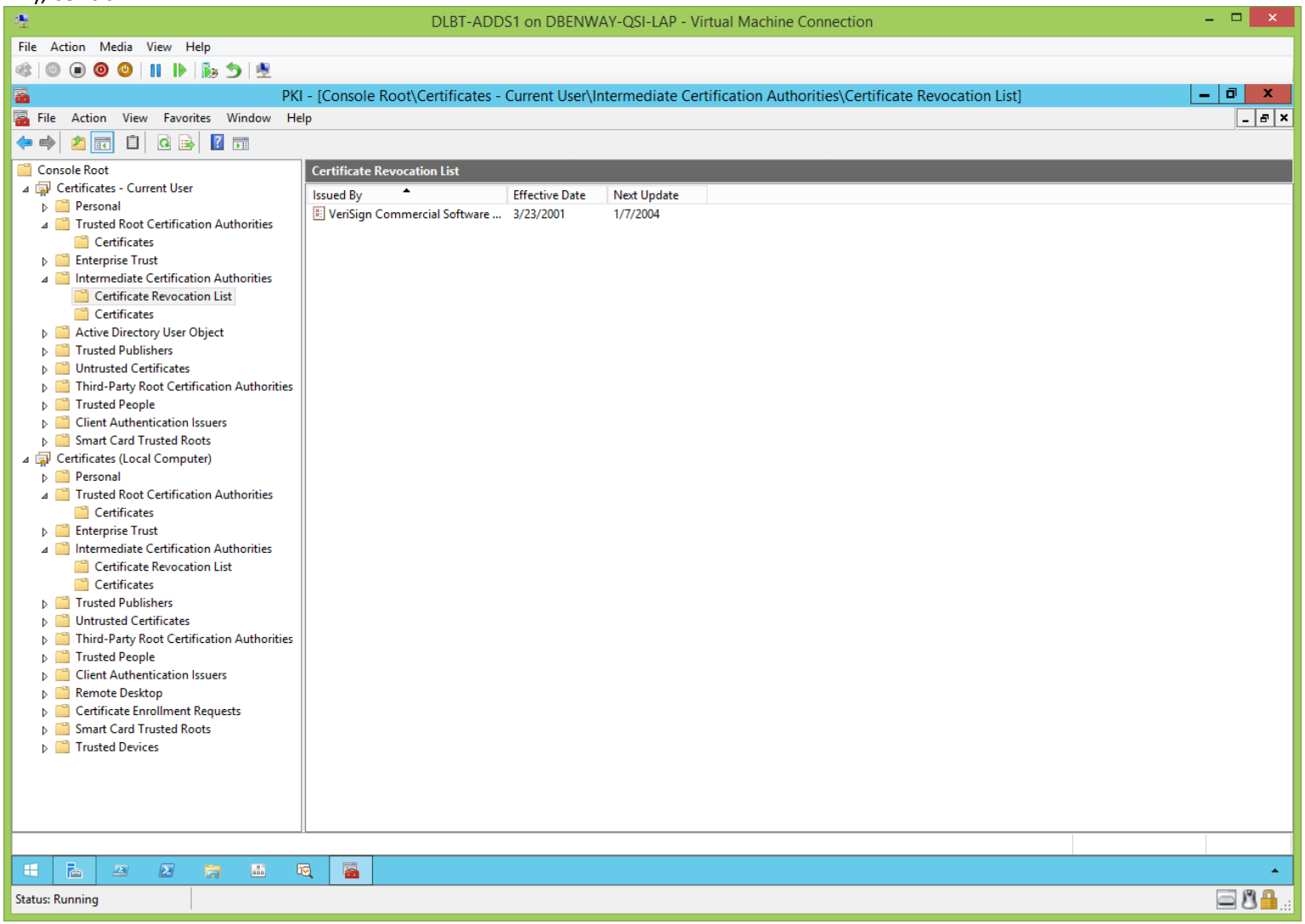
DC's Local Certificate Store (Before CertUtil.exe):

(jump to TOC)

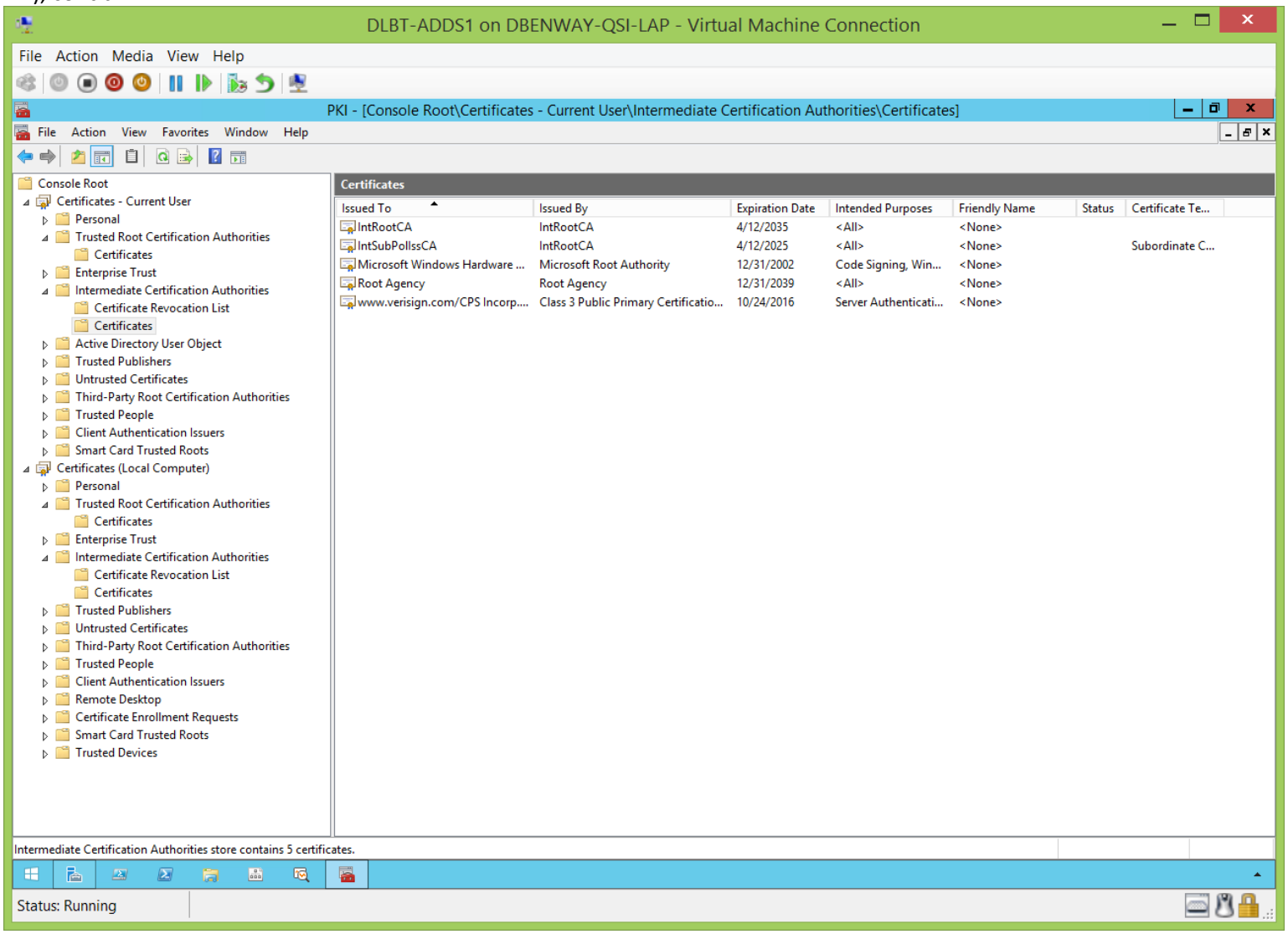
View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD):



View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:

DLBT-ADDS1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

PKI - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Smart Card Trusted Roots
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices

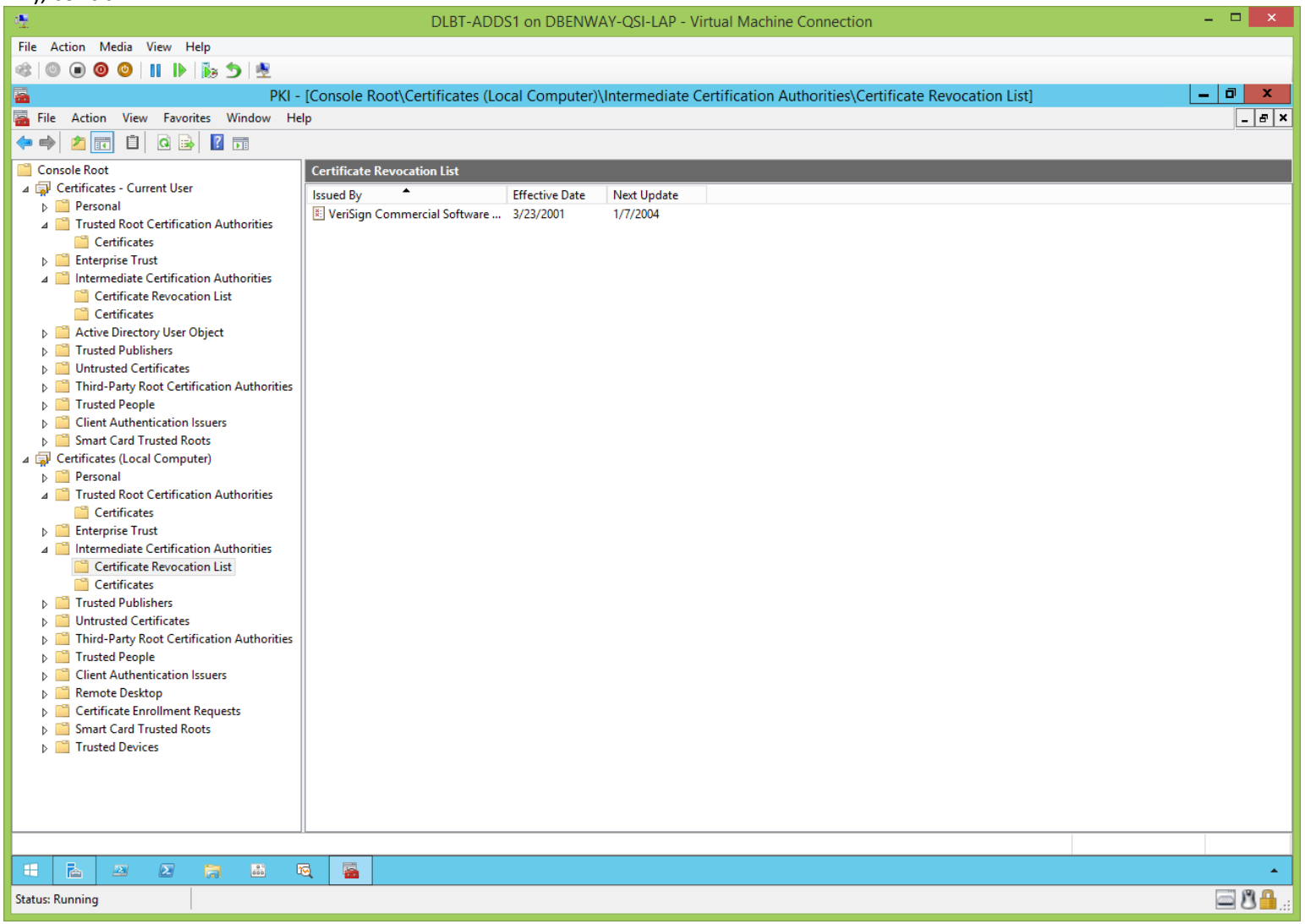
Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	Baltimore CyberTru...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert		
Entrust Root Certification Auth...	Entrust Root Certification Authority	11/27/2026	Server Authenticati...	Entrust		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...		
IntRootCA	IntRootCA	4/12/2035	<All>	<None>		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		

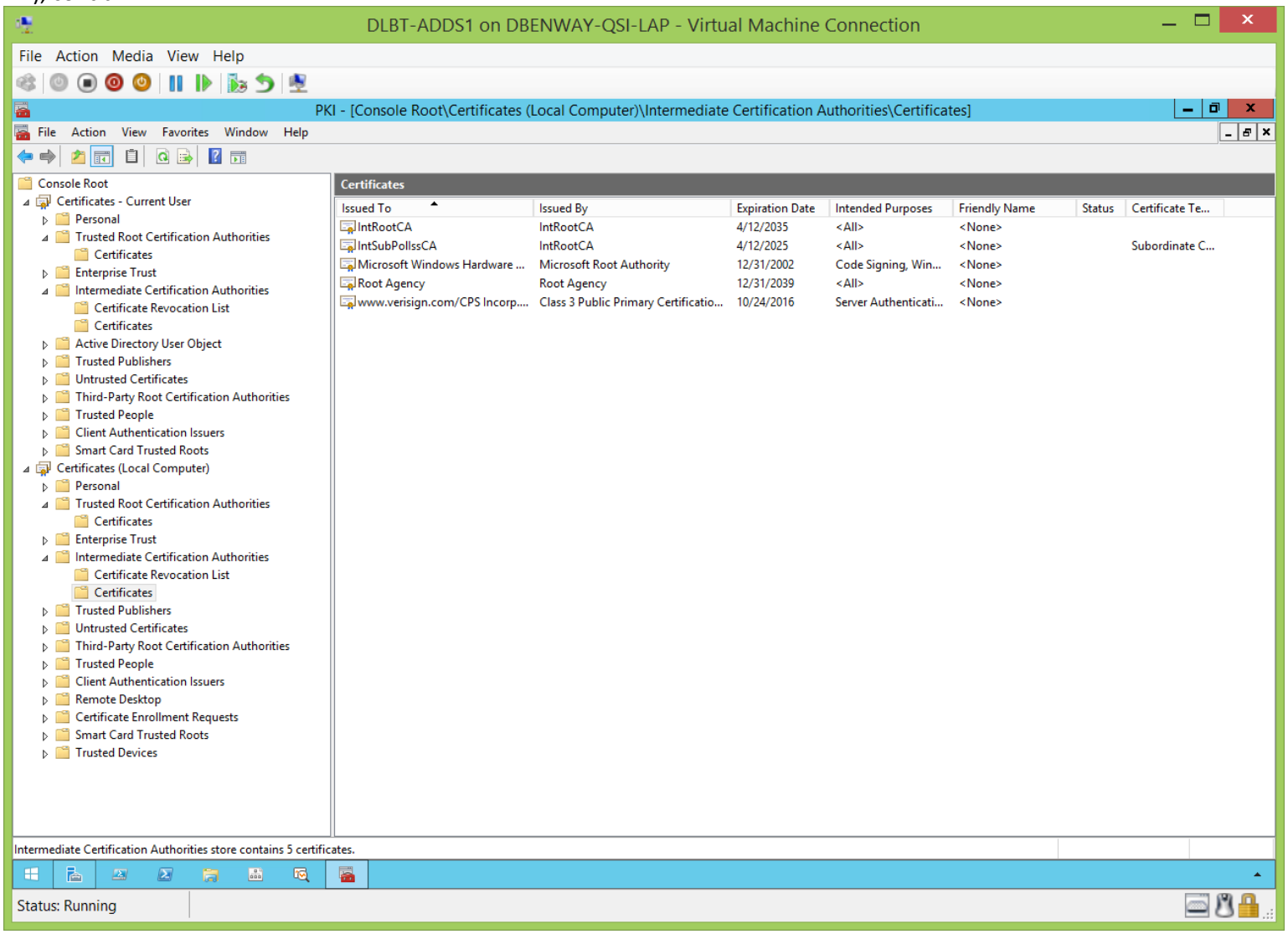
Trusted Root Certification Authorities store contains 16 certificates.

Status: Running

View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



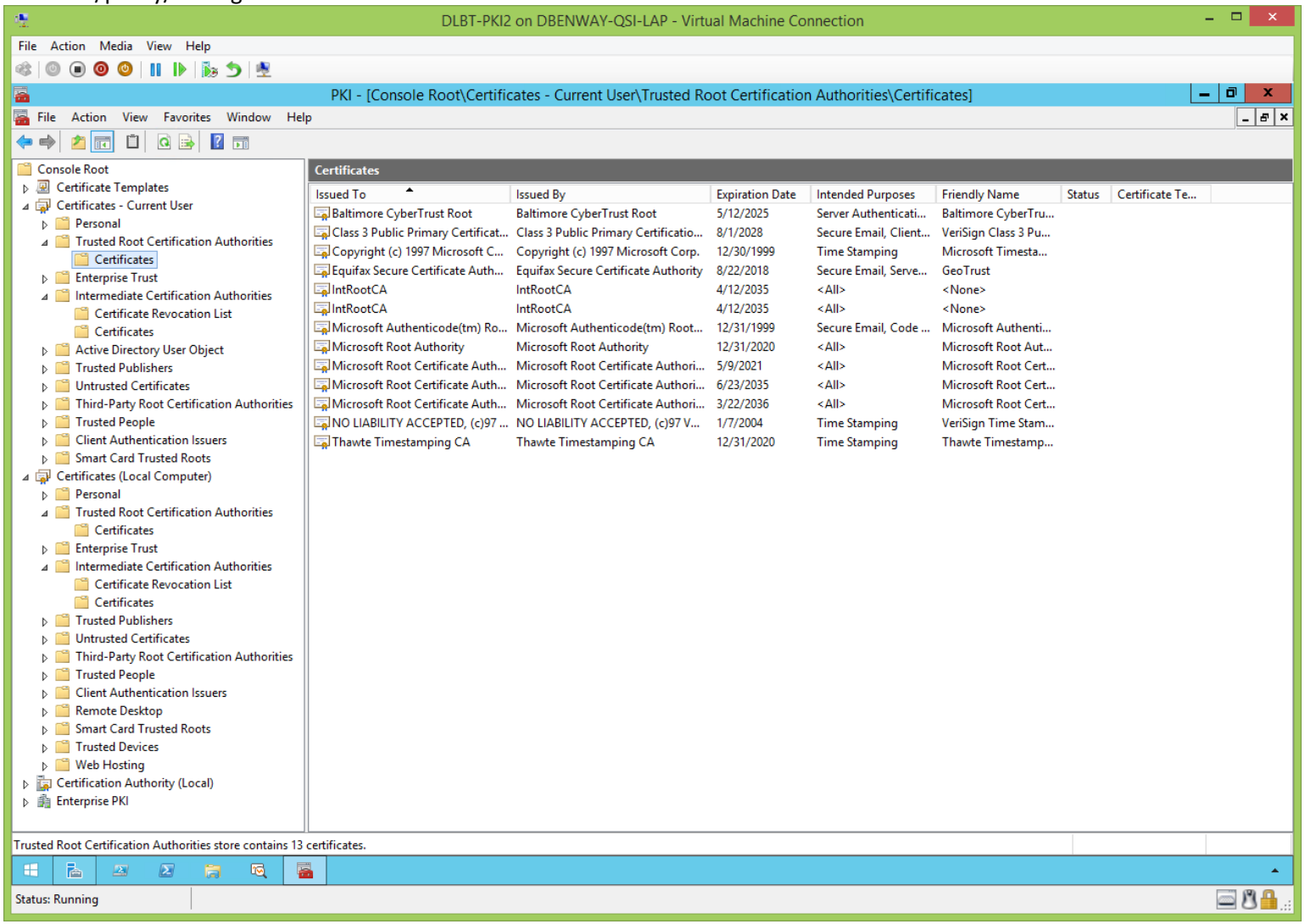
View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



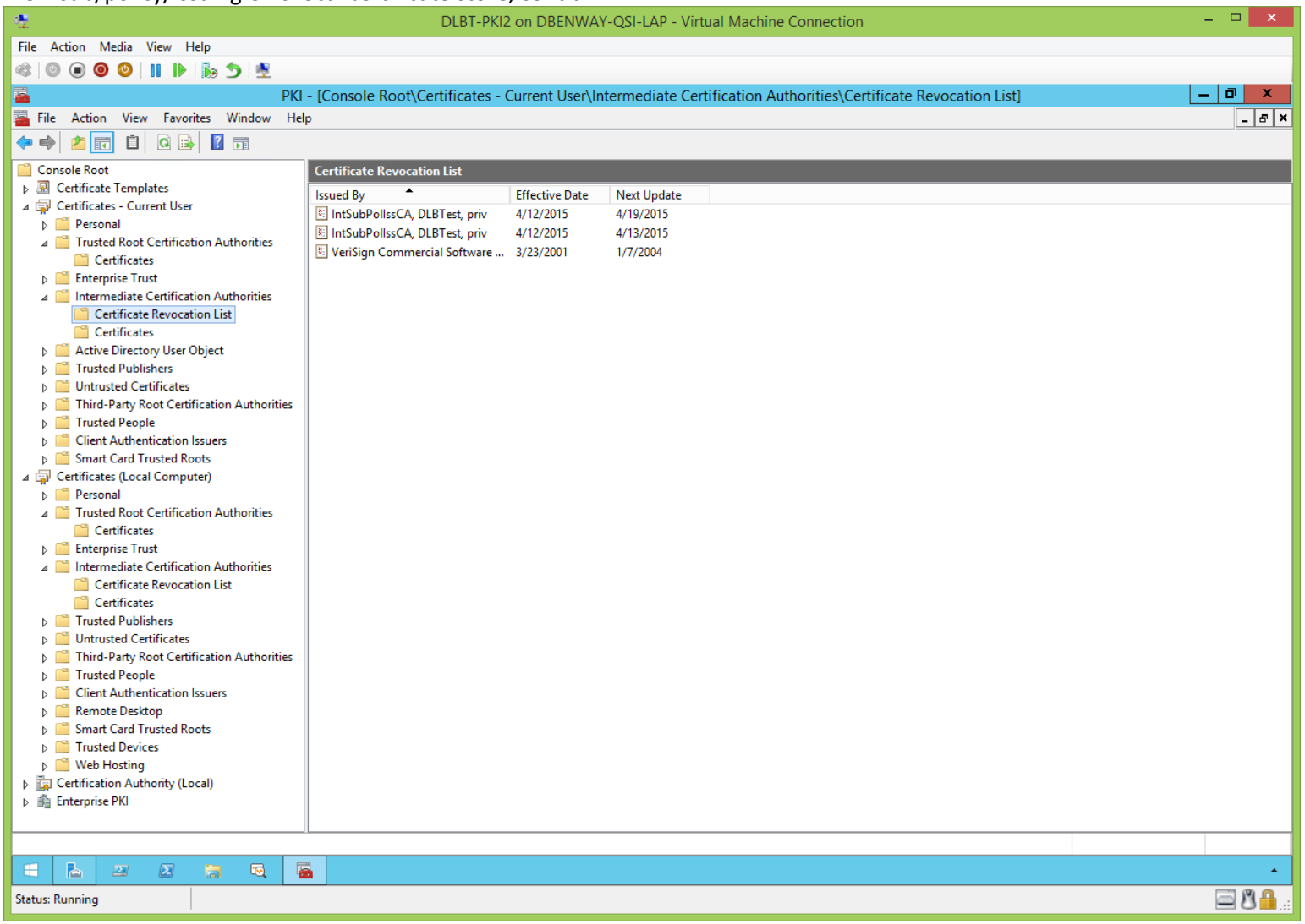
Sub/Policy/Issuing CA's Local Certificate Store (Before CertUtil.exe):

(jump to TOC)

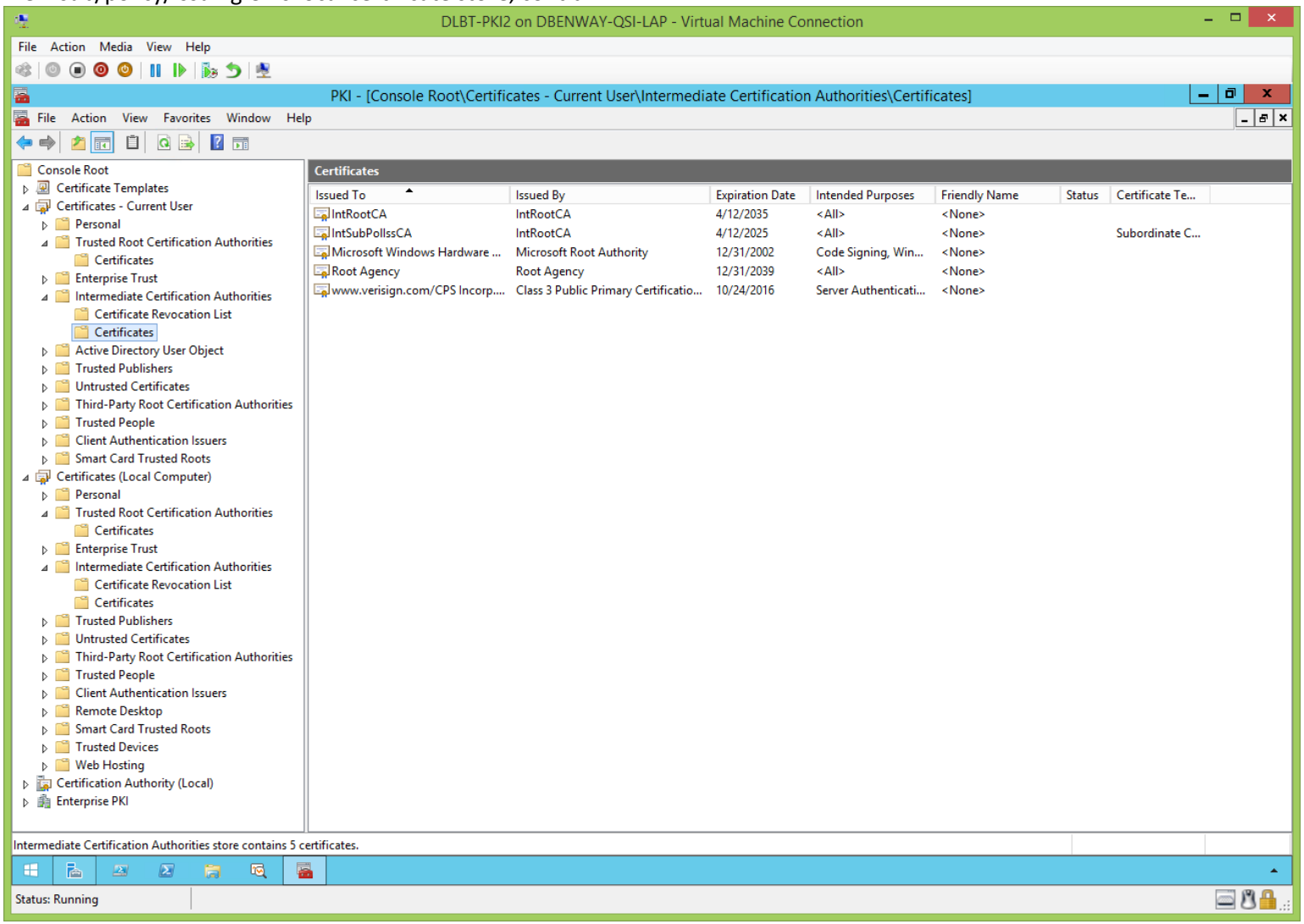
View sub/policy/issuing CA's local certificate store:



View sub/policy/issuing CA's local certificate store, cont'd:



View sub/policy/issuing CA's local certificate store, cont'd:



View sub/policy/issuing CA's local certificate store, cont'd:

DLBT-PKI2 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

PKI - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificate Templates
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Smart Card Trusted Roots
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Remote Desktop
    - Smart Card Trusted Roots
    - Trusted Devices
    - Web Hosting
  - Certification Authority (Local)
  - Enterprise PKI

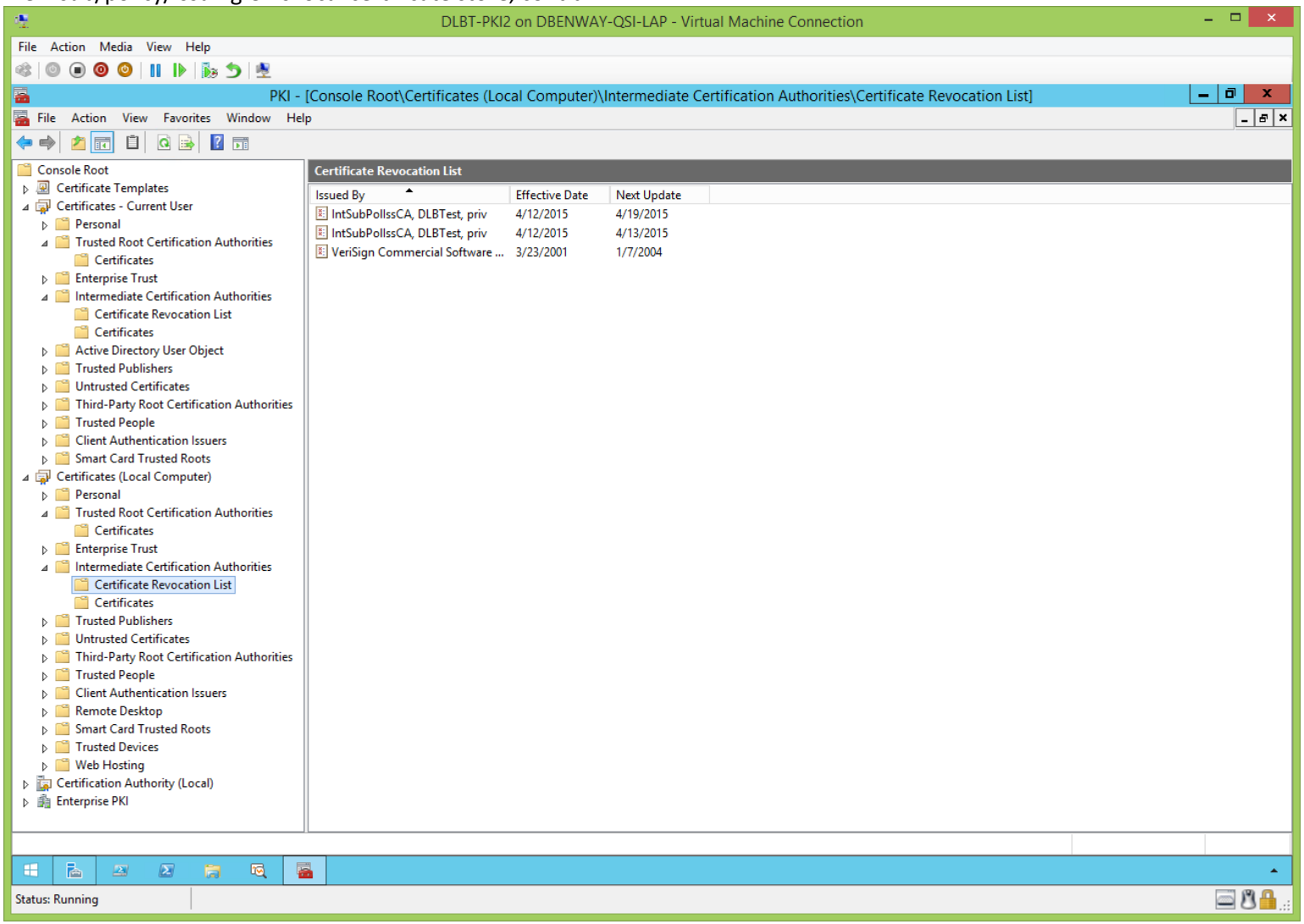
Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	Baltimore CyberTru...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
IntRootCA	IntRootCA	4/12/2035	<All>	<None>		
IntRootCA	IntRootCA	4/12/2035	<All>	<None>		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		

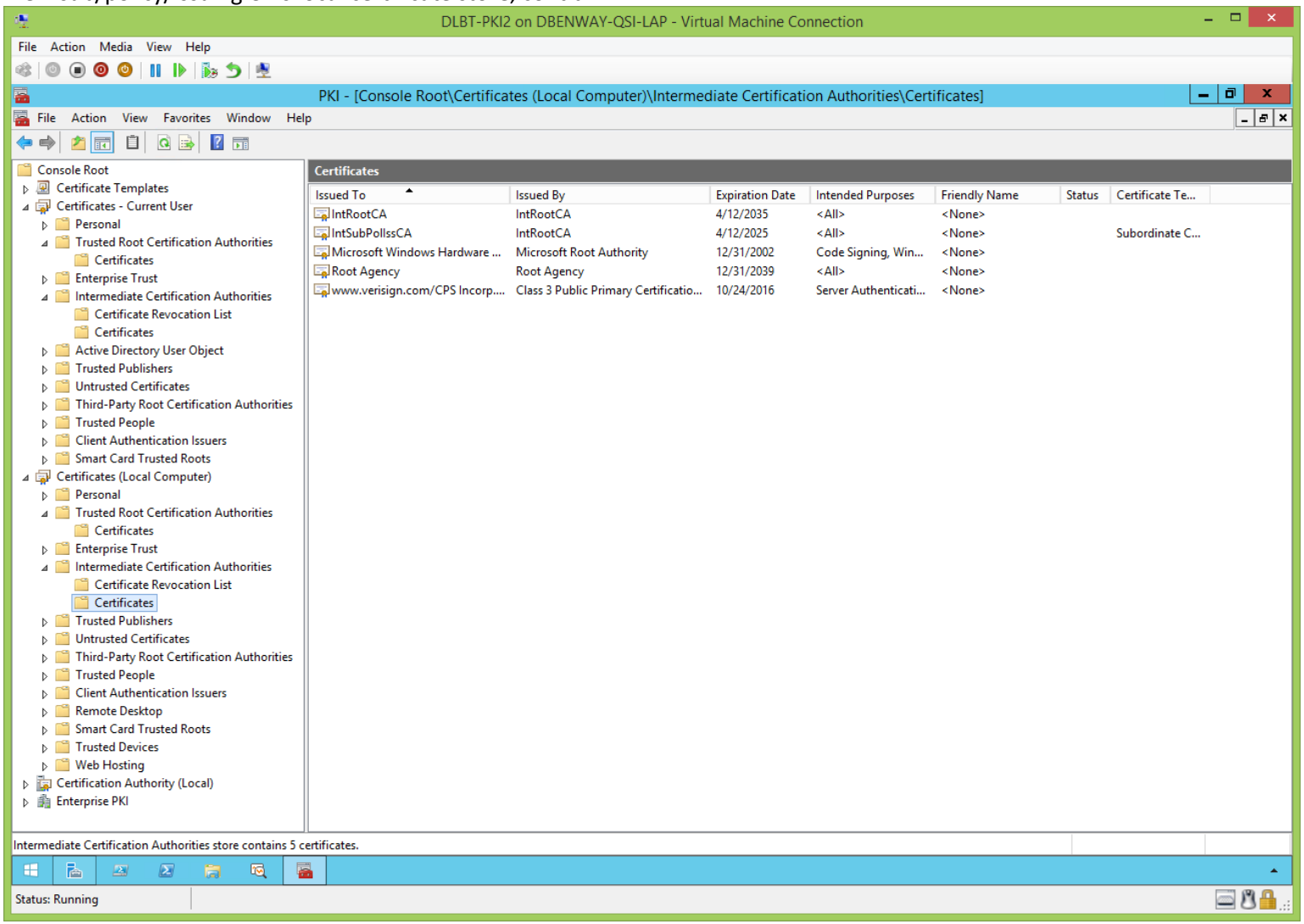
Trusted Root Certification Authorities store contains 13 certificates.

Status: Running

View sub/policy/issuing CA's local certificate store, cont'd:



View sub/policy/issuing CA's local certificate store, cont'd:



Sub/Policy/Issuing CA's CertUtil.exe:

(jump to TOC)

WARNING: This file of CertUtil.exe commands has a lot of important comments that need to be read and understood, or problems will arise.
Note: Because the CAPolicy.inf and Certutil.exe files in this document have been updated since initial publication, the values in this document's screenshots (such as registry settings, publication intervals, etc.) might not always reflect the values from these files.

Now we'll run CertUtil.exe commands from an Administrator command prompt on the sub/policy/issuing CA to configure the sub/policy/issuing CA (be sure to read and follow the steps in the REM comments):

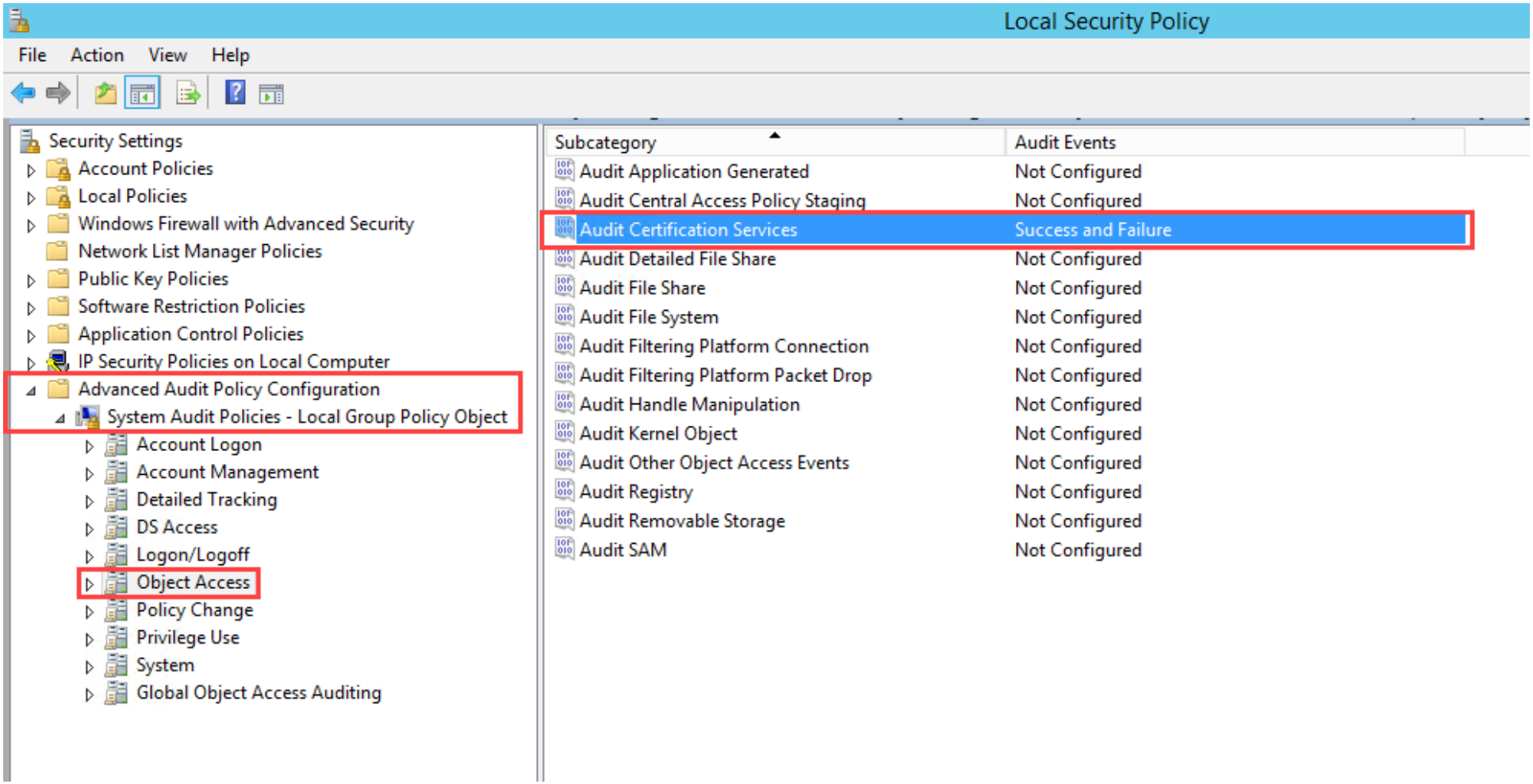
```
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
REM | CertUtil Sub/Policy/Issuing
REM |
REM | Run these commands interactively from an administrative command prompt.
REM | Note: Although this file is written in batch form it is not intended to be run as a batch file, but to have its chunks of code individually copied
REM | and pasted into a command line.
REM | Note: If you run this as a batch you'll need to replace % with %%, and maybe create a 'wait' when restarting services.
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Enable all auditing events for this sub/policy/issuing CA.
REM | Note: This can also be done from the 'Auditing' tab of this root CA's properties sheet in PKI.mmc, but better to turn it on early right after ADCS
REM | installation.
REM | Also be sure to use GPO or SecPol.msc to track Success and Failure in 'Advanced Audit Policy Configuration' > 'System Audit Policies' >
REM | 'Object Access' > Audit Certification Services.
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\AuditFilter 127

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Specify the Forest's configuration partition.
REM | This is only needed if citing LDAP URLs for AIA and/or CDP (which is no longer best practice!) but include it just in case.
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\DSConfigDN CN=Configuration,DC=DLBTest,DC=priv

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Set the validity period for the certificates this sub/policy/issuing CA issues (not for this sub/policy/issuing CA's certificate).
REM | Note: Standalone CAs configure validity periods for the certificates they issue in their registry, enterprise CAs do it in their templates (and
REM | if not there then it defaults to their registry).
REM | Note: The lowest certificates should have up to 5 years, so this sub/policy/issuing CA is 10, so the root CA is 20.
REM | Note: the validity period for the root CA's certificate is set during its ADCS installation wizard, and also in its CAPolicy.inf file's 'renewal'
REM | parameters
REM | Note: the validity period of this sub/policy/issuing CA's certificate is set during its ADCS installation wizard, and also in its CAPolicy.inf file's
REM | 'renewal' parameters
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\ValidityPeriodUnits 5
certUtil.exe -setReg CA\ValidityPeriod "years"

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Define the publication intervals for the base and the delta CRL this root CA generates.
REM | Note: The base and the delta CRL which control this sub/policy/issuing CA's certificate are published by the root CA per intervals set in the root
REM | CA's CDP extensions.
REM | Note: CRLOverlap parameters in CAPolicy.inf are ignored.
REM | Note: CRLOverlap cannot be greater than CRLPeriod.
```

```
REM | Note: This is a lab environment which is offline for extended periods, so these values are unusually large, and a delta CRL is not used.
REM | http://blogs.technet.com/b/xdot509/archive/2012/11/26/pki-design-considerations-certificate-revocation-and-crl-publishing-strategies.aspx
REM |        PKI Design Considerations: Certificate Revocation and CRL Publishing Strategies
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\CRLPeriodUnits 12
certUtil.exe -setReg CA\CRLPeriod "months"
certUtil.exe -setReg CA\CRLOverlapUnits 6
certUtil.exe -setReg CA\CRLOverlapPeriod "months"
REM |-----------------------------------------------
certUtil.exe -setReg CA\CRLDeltaPeriodUnits 0
certUtil.exe -setReg CA\CRLDeltaPeriod "days"
certUtil.exe -setReg CA\CRLDeltaOverlapUnits 0
certUtil.exe -setReg CA\CRLDeltaOverlapPeriod "days"

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Set the CDP extension URLs for the certificates this sub/policy/issuing CA issues (not for this sub/policy/issuing CA's certificate).
REM | This sub/policy/issuing CA will be issuing many certificates.
REM | You can use certUtil.exe or the GUI to set these URLs. Komar p. 115 describes the numeric codes used, but they should be (top to bottom):
REM | '1,8,4,2,64,128'.
REM | 65 means 1st and 5th checkboxes in this CA's CRL extensions GUI, 134 means 3rd, 4th, and 6th checkboxes in this CA's CRL extensions GUI.
REM | \n means new line (see Appendix A).
REM | %3 = CAName, %8 = CRLNameSuffix, %9 = DeltaCRLAllowed
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\CRLPublicationURLs
"65:%windir%\system32\CertSrv\CertEnroll\%3%8%9.crl\n65:C:\InetPub\PKI\CDP\%3%8%9.crl\n134:http://PKI.DLBTest.priv/CDP/%3%8%9.crl"

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Set the AIA extension URLs for the certificates this sub/policy/issuing CA issues (not for this sub/policy/issuing CA's certificate).
REM | This sub/policy/issuing CA will be issuing many certificates.
REM | You can use certUtil.exe or the GUI to set these URLs. Komar p. 116 describes the numeric codes used, but '1' doesn't seem valid?
REM | 0 means no checkboxes in this CA's AIA extensions GUI, 2 means the 1st checkbox in this CA's AIA extensions GUI.
REM | \n means new line (see Appendix A).
REM | %1 = ServerDNSName, %3 = CAName, %4 = CertificateName
REM | Note: most sources recommend not using the '%1_' in the AIA extension URLs to create security through obscurity (see Appendix B).
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -setReg CA\CACertPublicationURLs "0:%windir%\system32\CertSrv\CertEnroll\%3%4.crt\n0:C:\InetPub\PKI\AIA\%3%4.crt\n2:http://PKI.DLBTest.priv/AIA/%3%4.crt"

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM |Restart Certificate Services so the above changes take effect
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
net stop CertSvc & net start CertSvc

REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
REM | Publish this CA's base CRL and delta CRL (to whatever this CA's CDP extensions specify).
REM |-----------------------------------------------------------------------------------------------------------------------------------------------------------
certUtil.exe -CRL
```

Finish Enabling Auditing on the Sub/Policy/Issuing CA (After CertUtil.exe):

(jump to TOC)

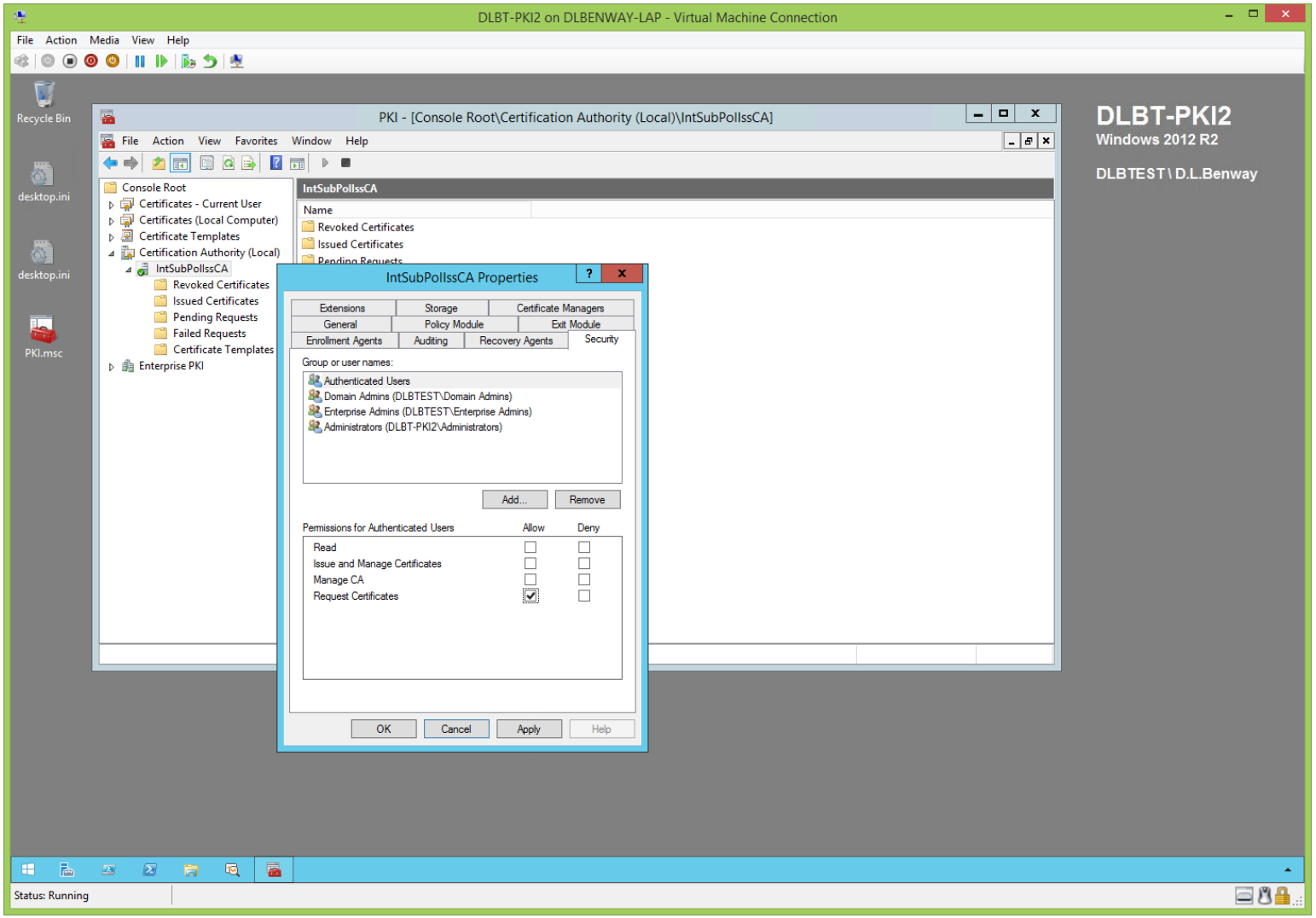
In addition to the 'certUtil.exe -setReg CA\AuditFilter 127' command, finish enabling auditing on the sub/pol/issuing CA preferably by using GPO, or less preferably by using SecPol.msc as follows:



Sub/Policy/Issuing CA's Right to Issue Certificates:

(jump to TOC)

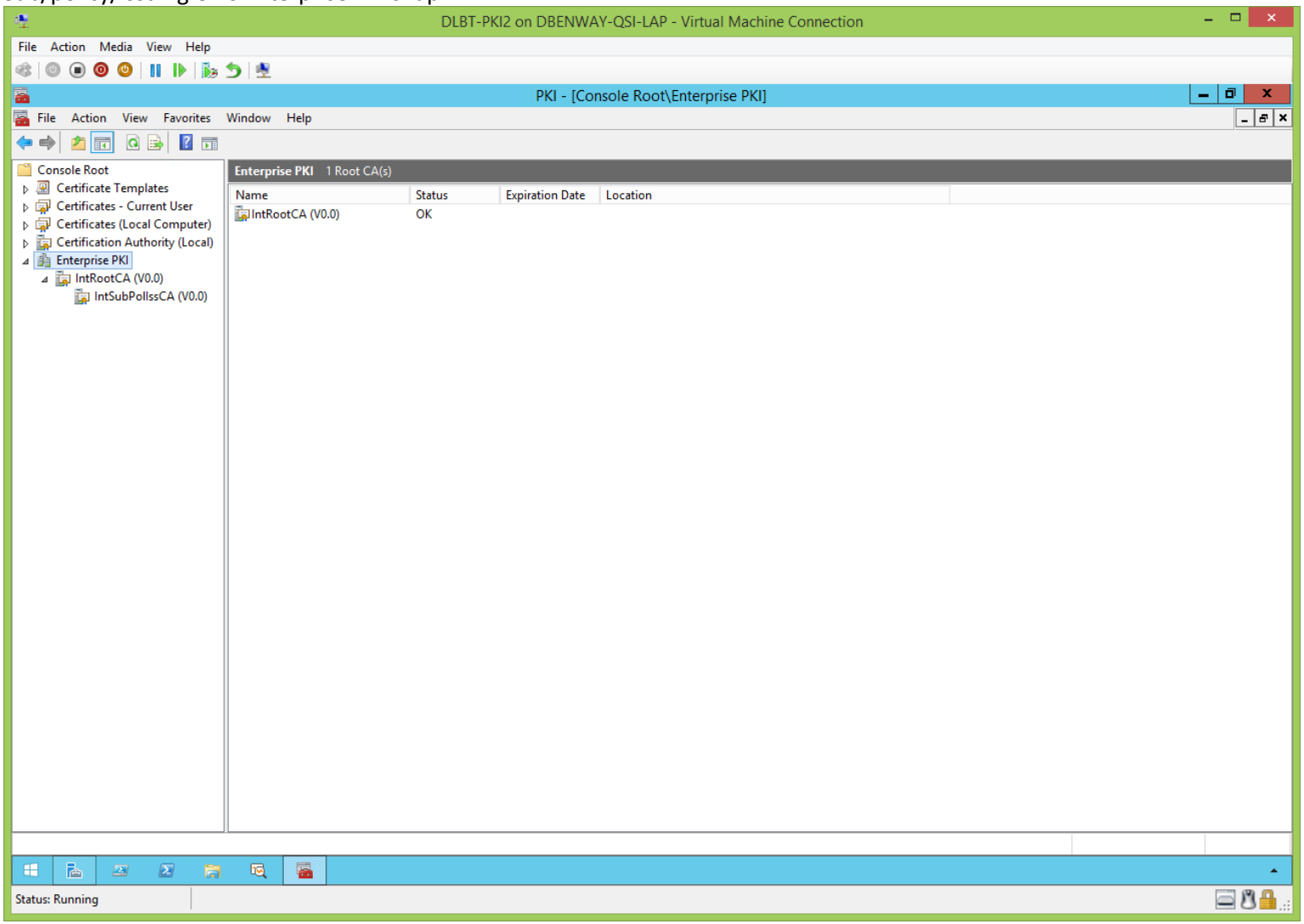
Now that the sub/policy/issuing CA is fully configured, give 'Authenticated Users' the right on the sub/policy/issuing CA to 'Request Certificates'.



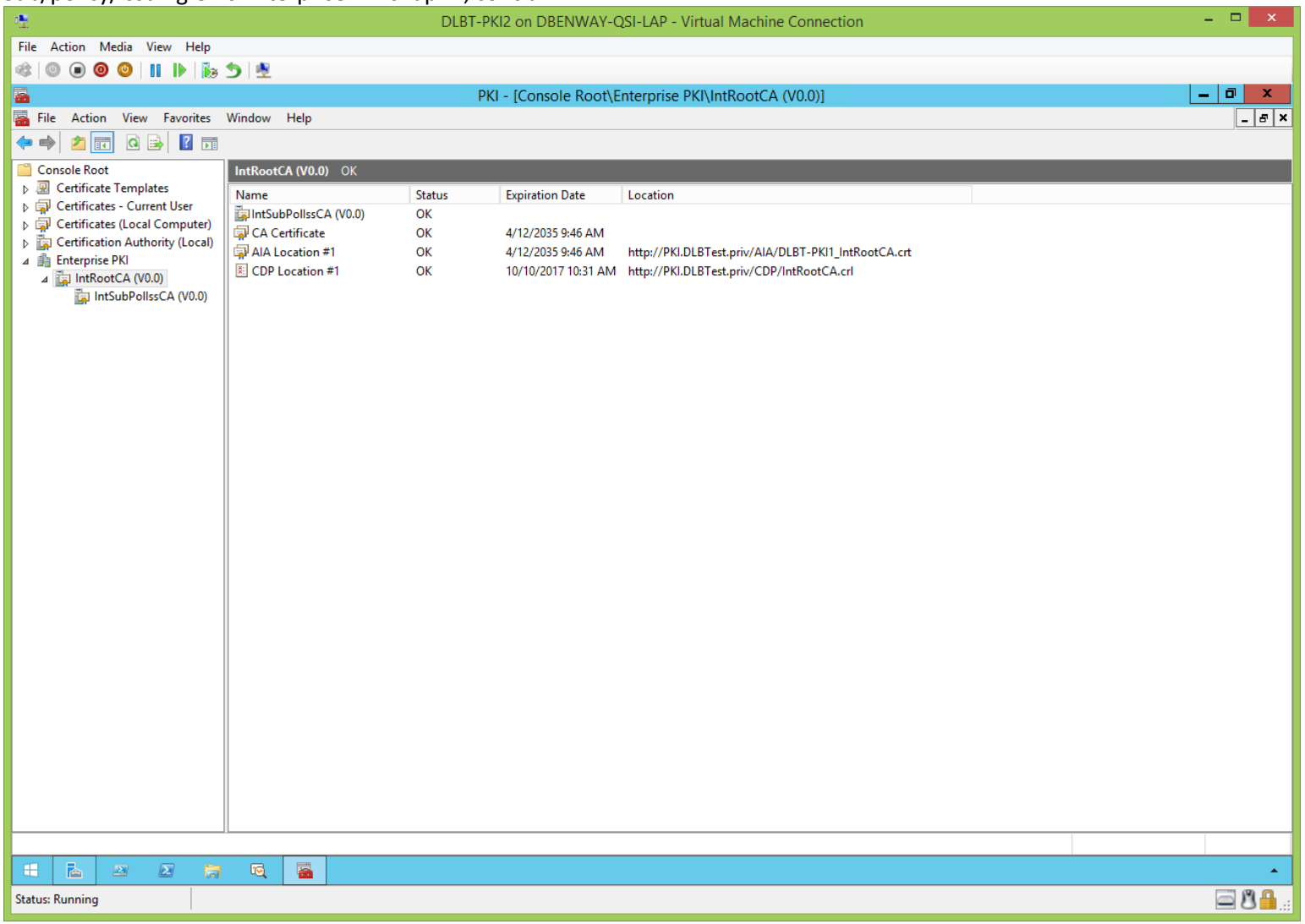
Sub/Policy/Issuing CA's Enterprise PKI Snap-In (After CertUtil.exe):

(jump to TOC)

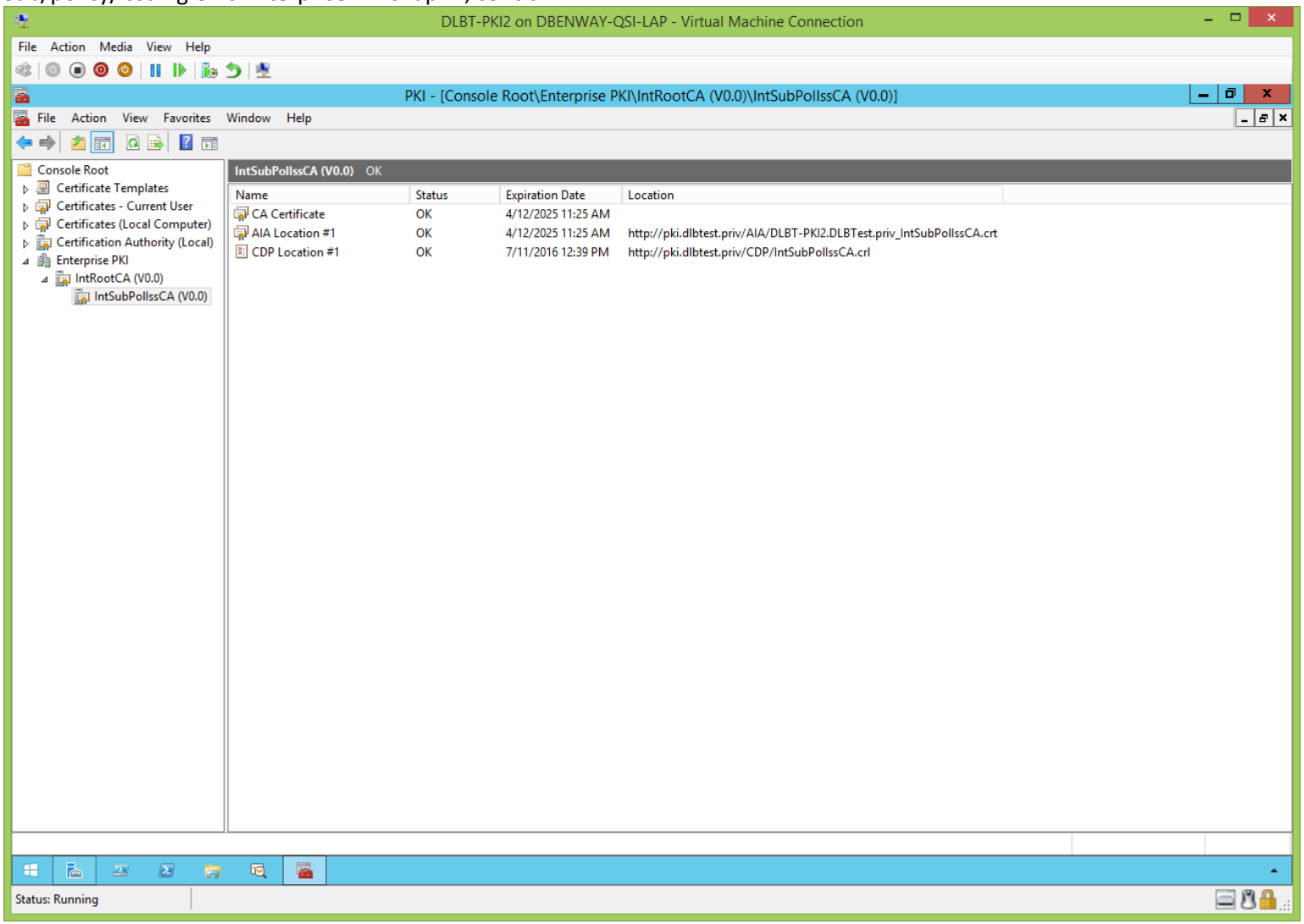
Sub/policy/issuing CA's Enterprise PKI snap-in:



Sub/policy/issuing CA's Enterprise PKI snap-in, cont'd:



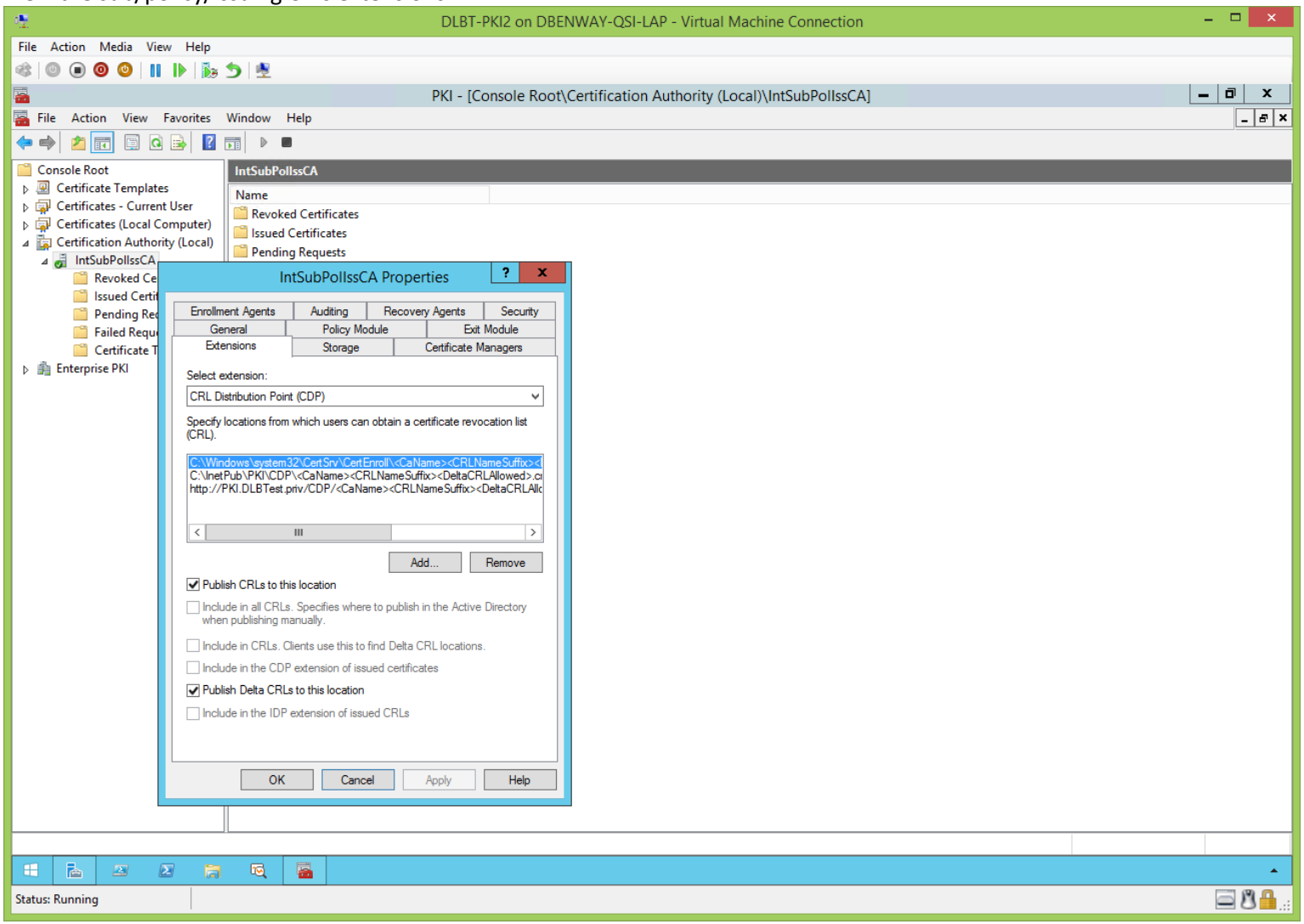
Sub/policy/issuing CA's Enterprise PKI snap-in, cont'd:



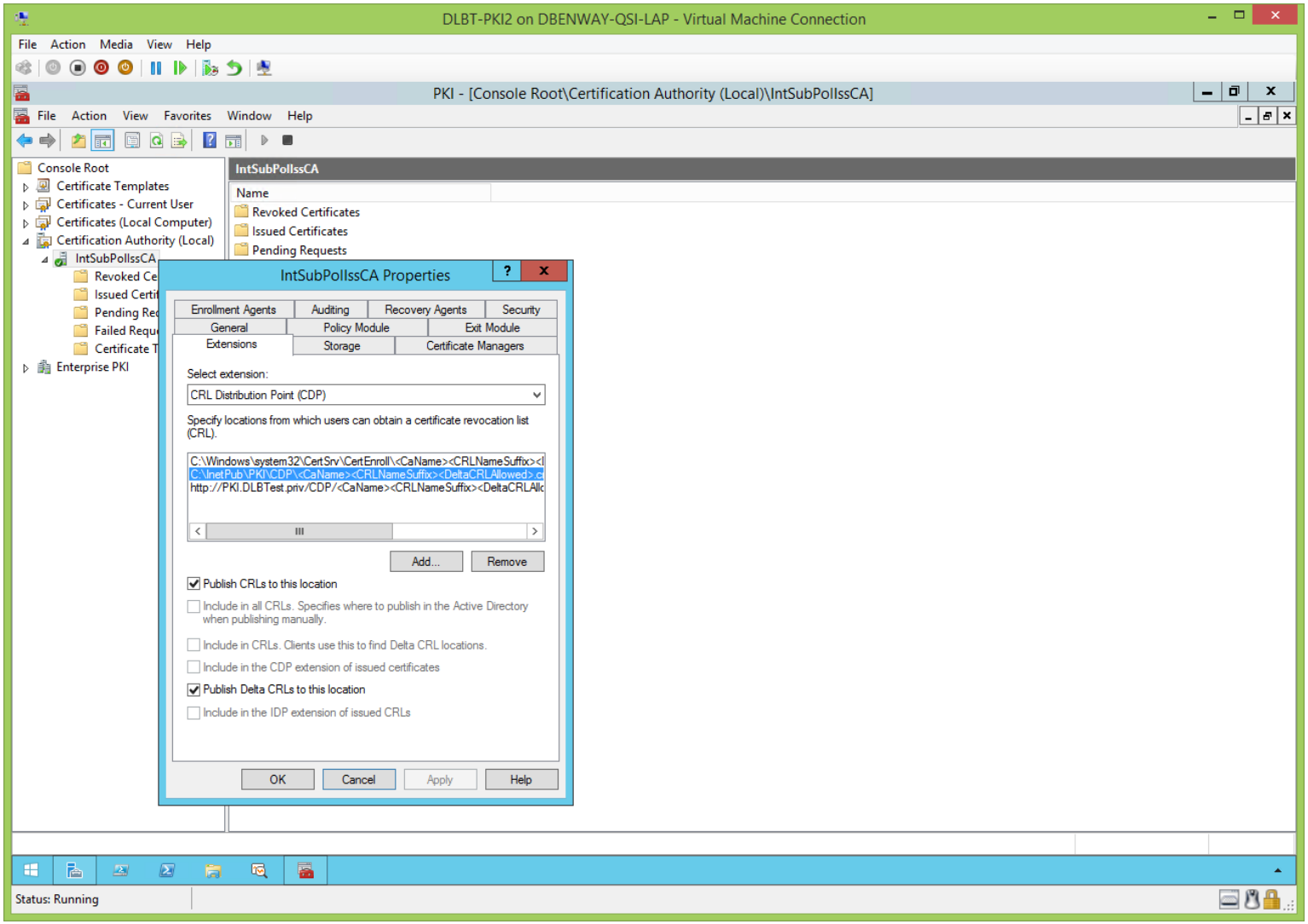
Sub/Policy/Issuing CA's Extensions (After CertUtil.exe):

(jump to TOC)

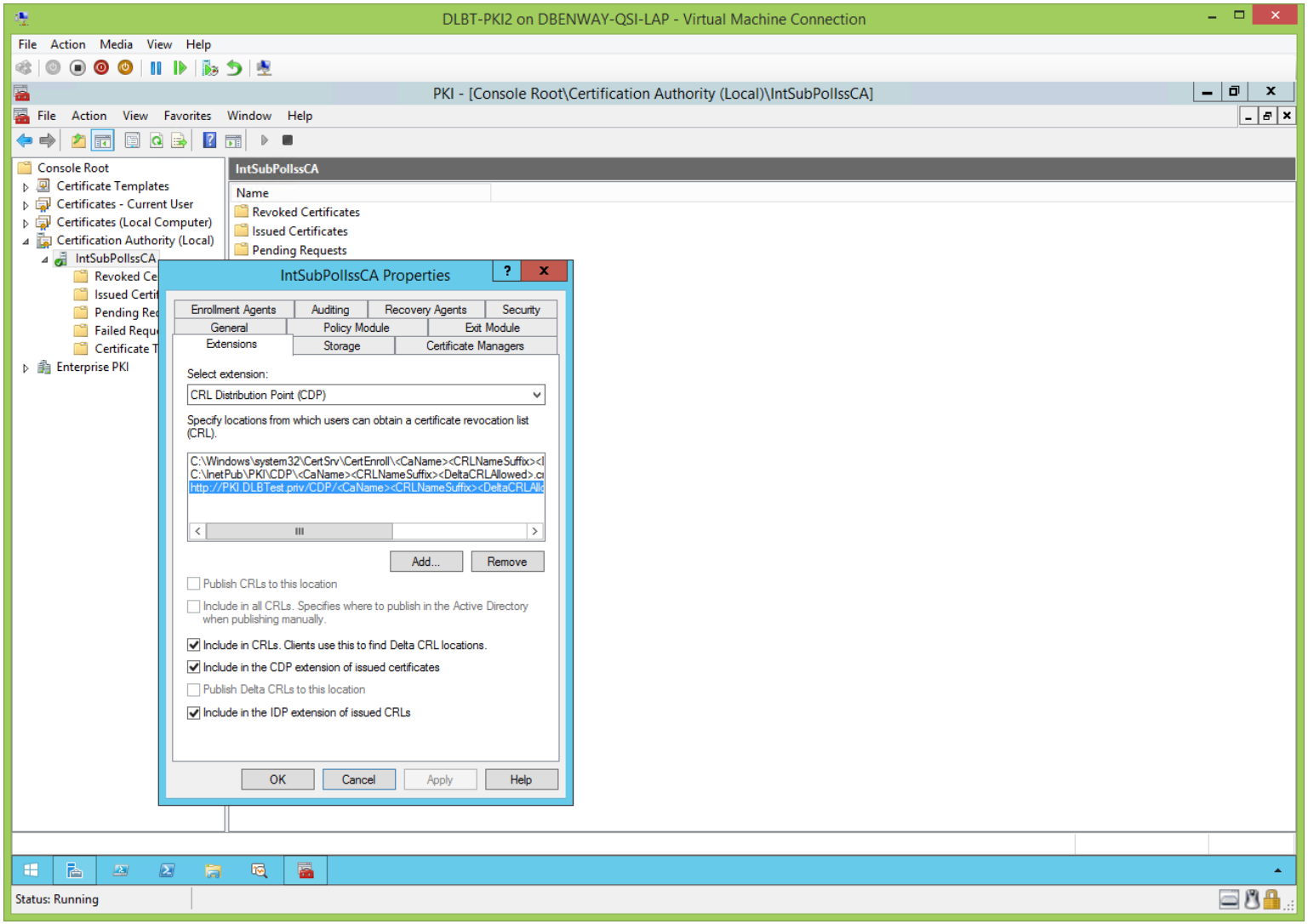
View the sub/policy/issuing CA's extensions:



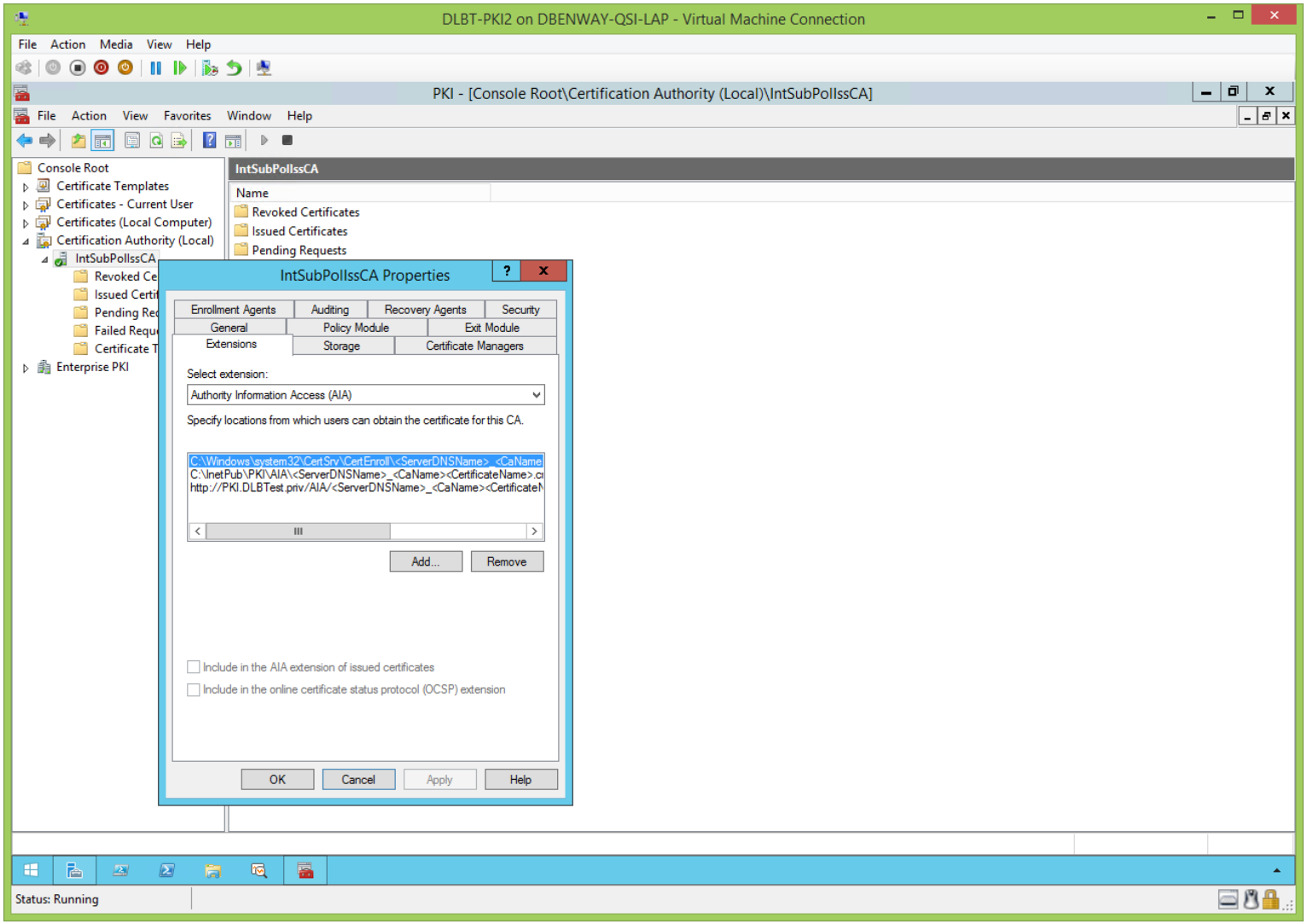
View the sub/policy/issuing CA's extensions, cont'd:



View the sub/policy/issuing CA's extensions, cont'd:

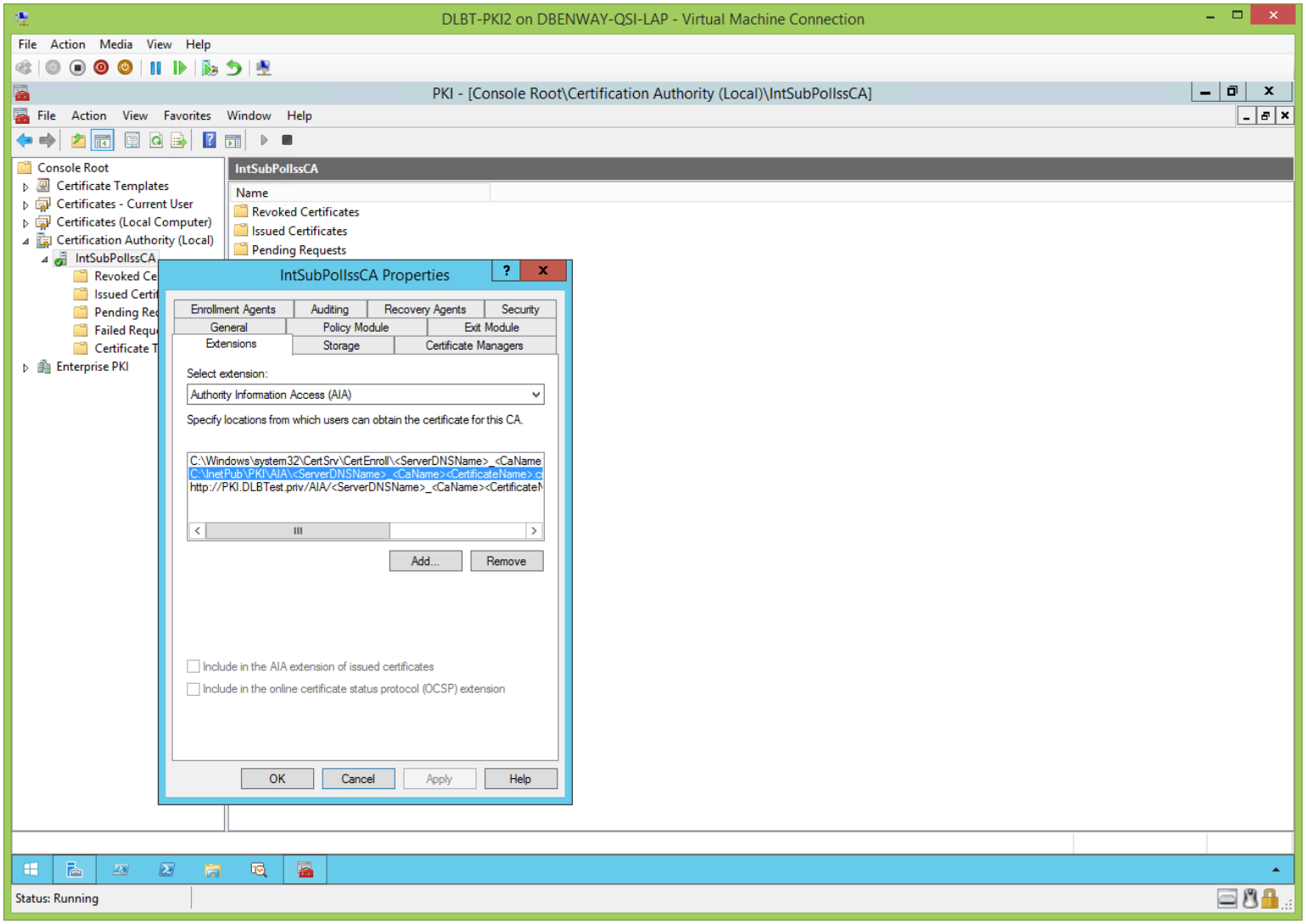


View the sub/policy/issuing CA's extensions, cont'd:



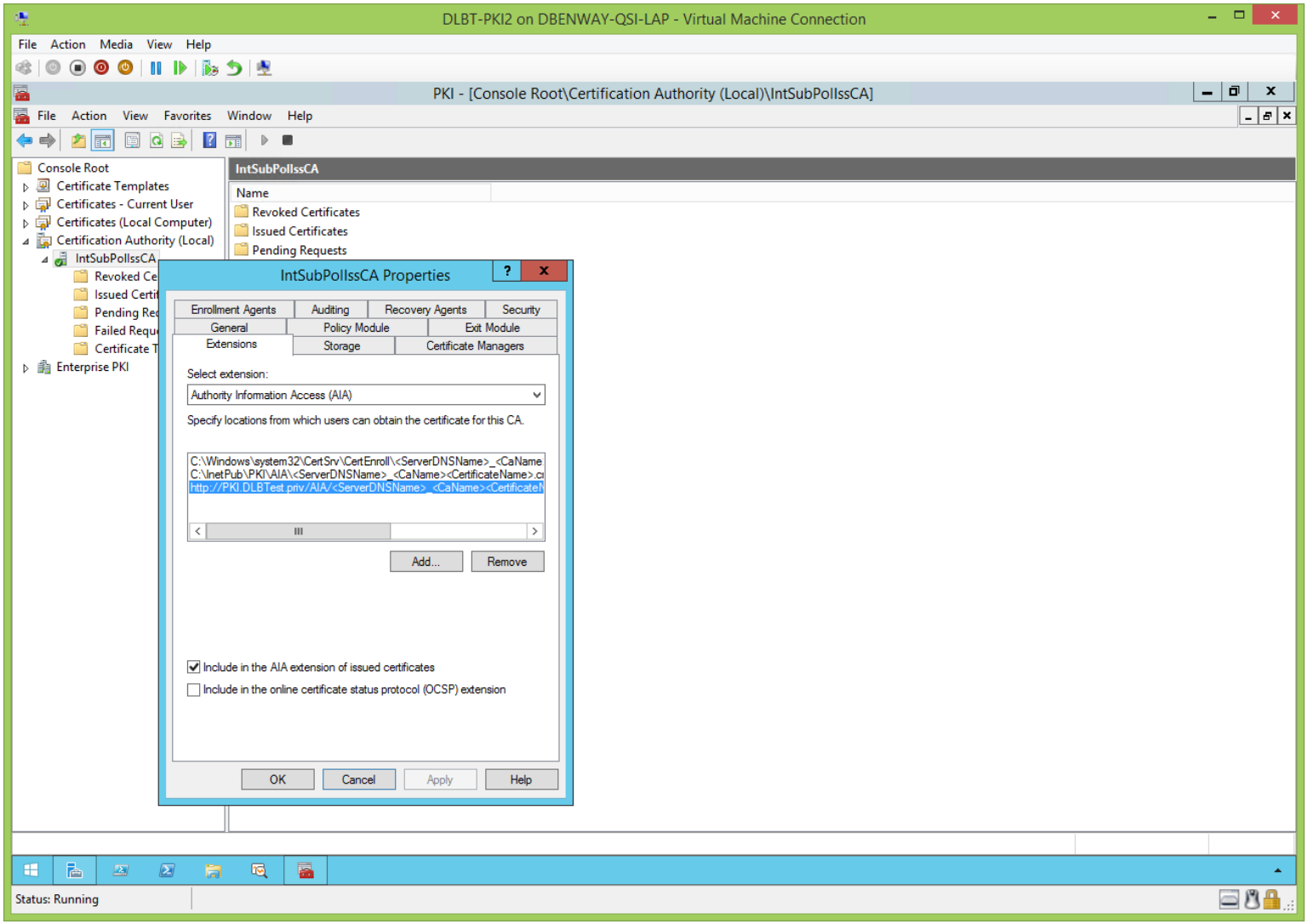
Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's certificate filename contains the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

View the sub/policy/issuing CA's extensions, cont'd:



Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's certificate filename contains the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

View the sub/policy/issuing CA's extensions, cont'd:

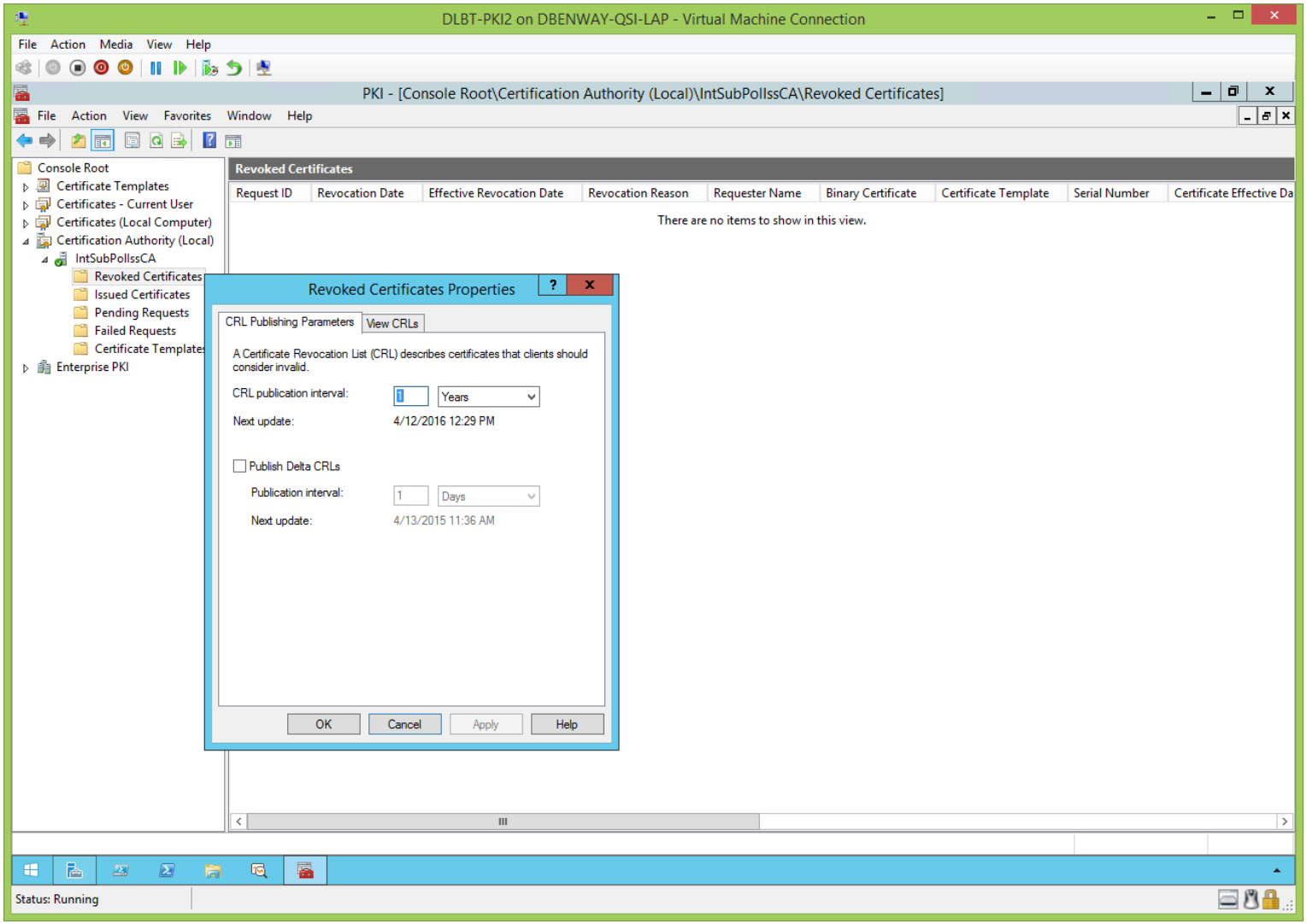


Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

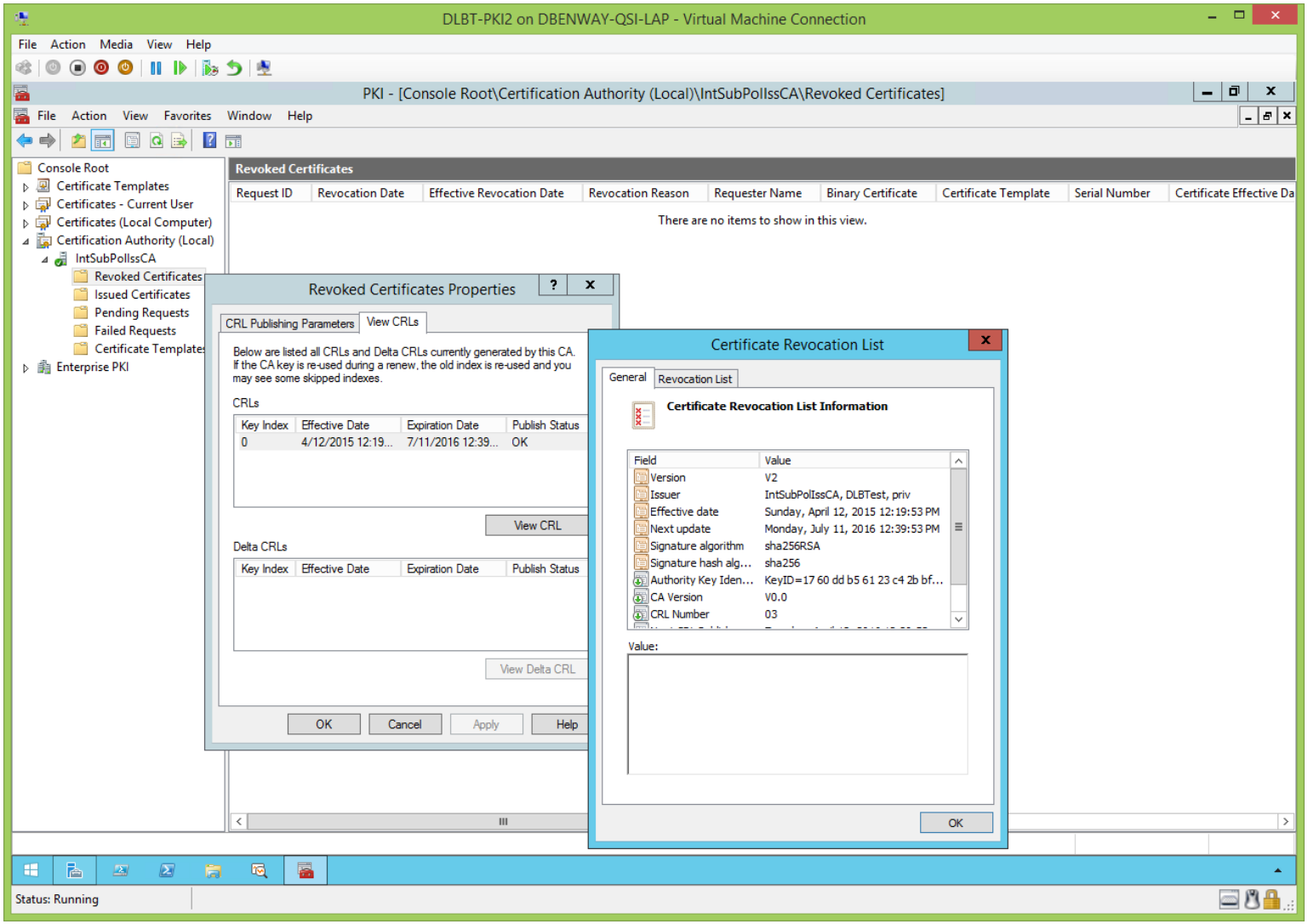
Sub/Policy/Issuing CA's CRLs (After CertUtil.exe):

(jump to TOC)

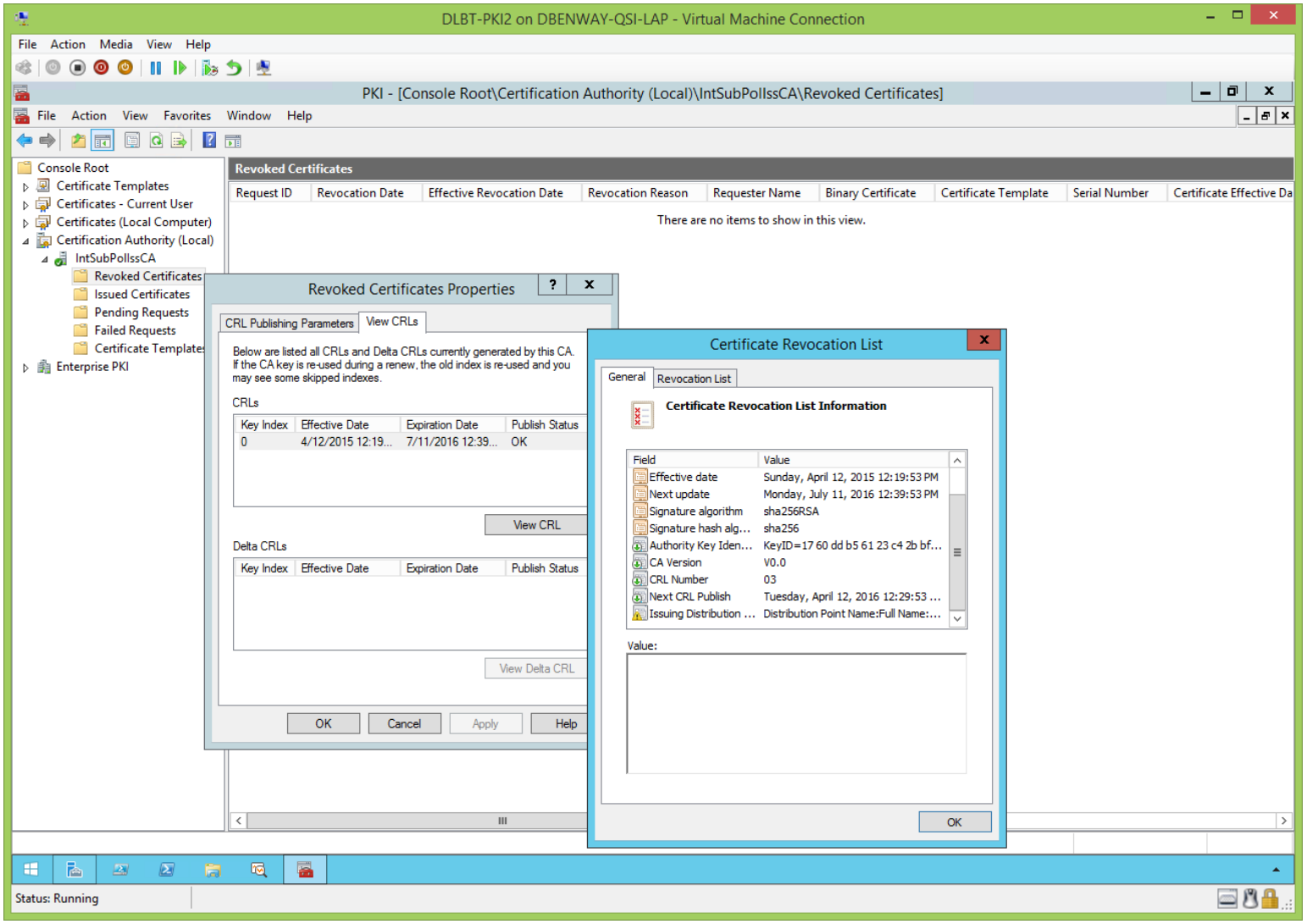
View the sub/policy/issuing CA's CRL properties:



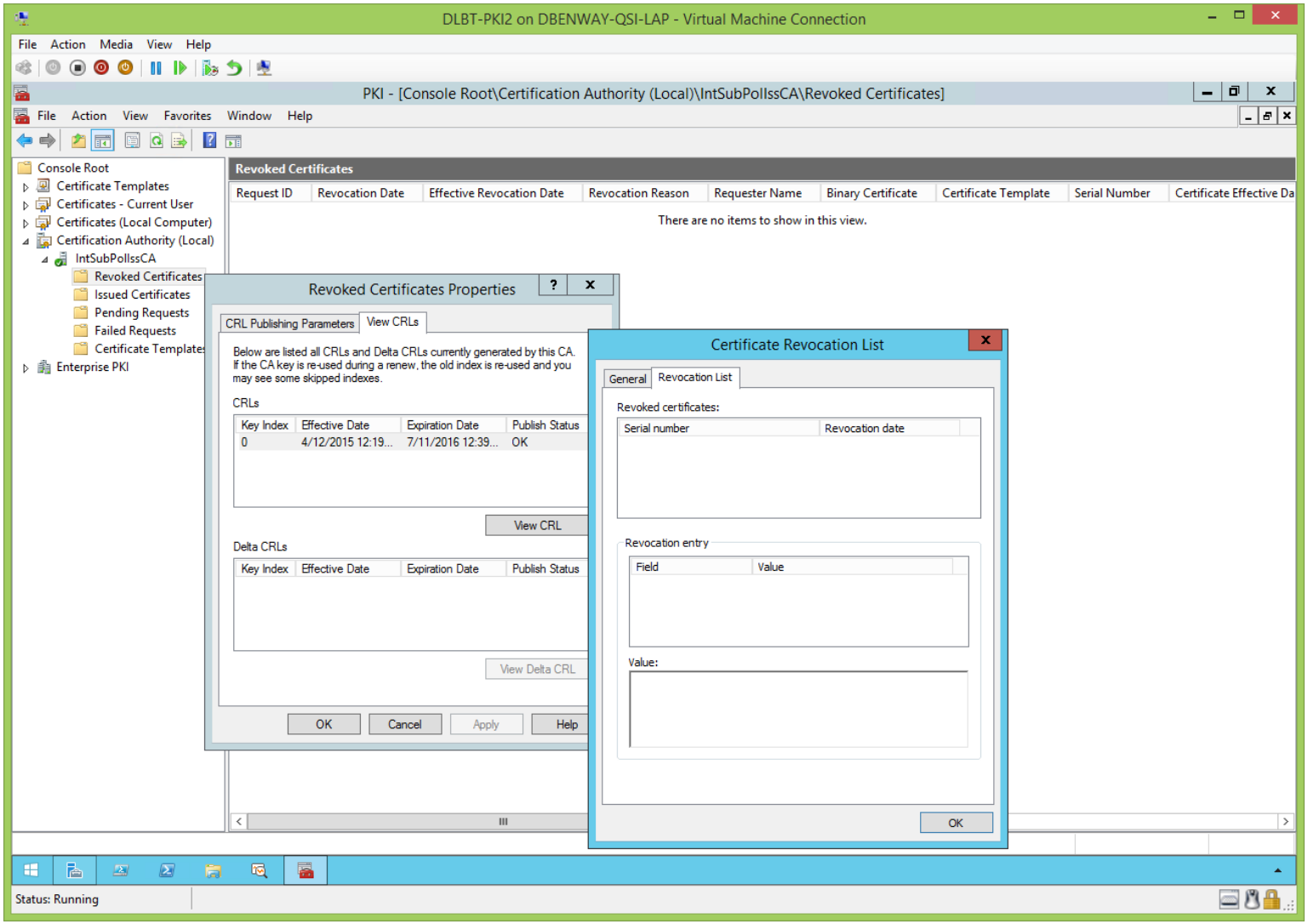
View the sub/policy/issuing CA's CRL properties, cont'd:



View the sub/policy/issuing CA's CRL properties, cont'd:



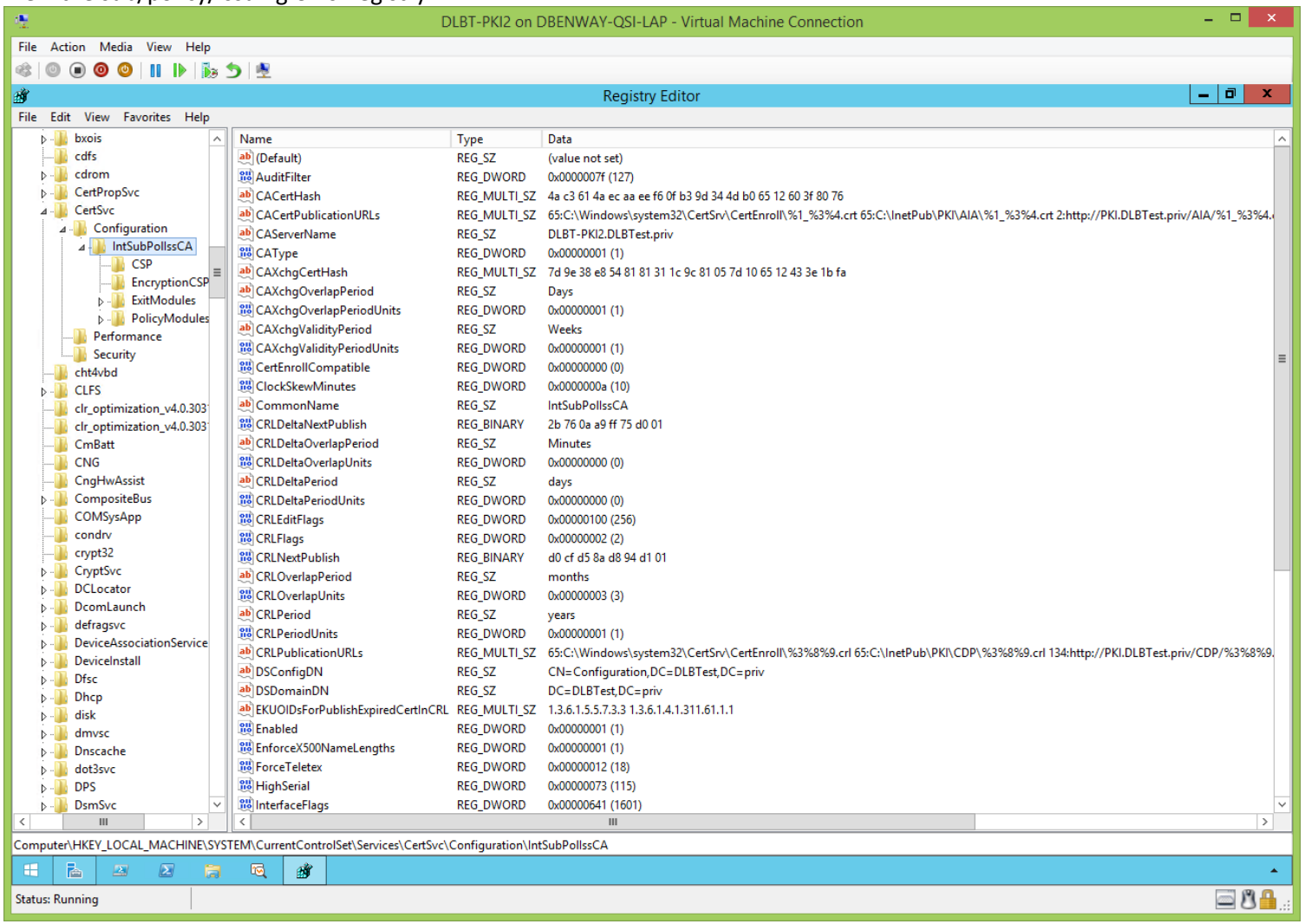
View the sub/policy/issuing CA's CRL properties, cont'd:



Sub/Policy/Issuing Registry (After CertUtil.exe):

(jump to TOC)

View the sub/policy/issuing CA's Registry:



Note: this lab was built using %1_ in the CertUtil.exe commands for clarity, so the CA's certificate filename contains the CA's server name. This is not best practice in the enterprise. The %1_ has been removed from the CertUtil.exe commands in this document to avoid accidental usage of that variable in non-lab environments.

View the sub/policy/issuing CA's Registry, cont'd:

DLBT-PKI2 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

Registry Editor

File Edit View Favorites Help

bxois
cdfs
cdrom
CertPropSvc
CertSvc
Configuration
IntSubPolIssCA
CSP
EncryptionCSP
ExitModules
PolicyModules
Performance
Security
cht4vbd
CLFS
clr_optimization_v4.0.303
clr_optimization_v4.0.303
CmBatt
CNG
CngHwAssist
CompositeBus
COMSysApp
condrv
crypt32
CryptSvc
DCLocator
DcomLaunch
defragsvc
DeviceAssociationService
DeviceInstall
Dfsc
Dhcp
disk
dmvsc
Dnscache
dot3svc
DPS
DsmSvc

Name	Type	Data
CRLDeltaPeriodUnits	REG_DWORD	0x00000000 (0)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	d0 cf d5 8a d8 94 d1 01
CRLOverlapPeriod	REG_SZ	months
CRLOverlapUnits	REG_DWORD	0x00000003 (3)
CRLPeriod	REG_SZ	years
CRLPeriodUnits	REG_DWORD	0x00000001 (1)
CRLPublicationURLs	REG_MULTI_SZ	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl 65:C:\InetPub\PKI\CDP\%3%8%9.crl 134:http://PKI.DLBTest.priv/CDP/%3%8%9.
DSConfigDN	REG_SZ	CN=Configuration,DC=DLBTest,DC=priv
DSDomainDN	REG_SZ	DC=DLBTest,DC=priv
EKUOIDsForPublishExpiredCertInCRL	REG_MULTI_SZ	1.3.6.1.5.5.7.3.3 1.3.6.1.4.1.311.61.1.1
Enabled	REG_DWORD	0x00000001 (1)
EnforceX500NameLengths	REG_DWORD	0x00000001 (1)
ForceTeletex	REG_DWORD	0x00000012 (18)
HighSerial	REG_DWORD	0x00000073 (115)
InterfaceFlags	REG_DWORD	0x00000641 (1601)
KRACertCount	REG_DWORD	0x00000000 (0)
KRACertHash	REG_MULTI_SZ	
KRAFlags	REG_DWORD	0x00000000 (0)
LogLevel	REG_DWORD	0x00000003 (3)
MaxIncomingAllocSize	REG_DWORD	0x00010000 (65536)
MaxIncomingMessageSize	REG_DWORD	0x00010000 (65536)
PolicyFlags	REG_DWORD	0x00000000 (0)
RequestFileName	REG_SZ	C:\DLBT-PKI2.DLBTest.priv_DLBTest-DLBT-PKI2-CA%4.req
Security	REG_BINARY	01 00 14 84 20 01 00 00 30 01 00 00 14 00 00 00 44 00 00 00 02 00 30 00 02 00 00 00 02 c0 14 00 ff ff 00 00 01 01 00 00 00 00 00 01 00 00 00 00 02
SetupStatus	REG_DWORD	0x00000001 (1)
SignedAttributes	REG_MULTI_SZ	RequesterName
SubjectTemplate	REG_MULTI_SZ	EMail CommonName OrganizationalUnit Organization Locality State DomainComponent Country
UseDS	REG_DWORD	0x00000001 (1)
ValidityPeriod	REG_SZ	years
ValidityPeriodUnits	REG_DWORD	0x00000005 (5)
ViewAgeMinutes	REG_DWORD	0x00000010 (16)
ViewIdleMinutes	REG_DWORD	0x00000008 (8)

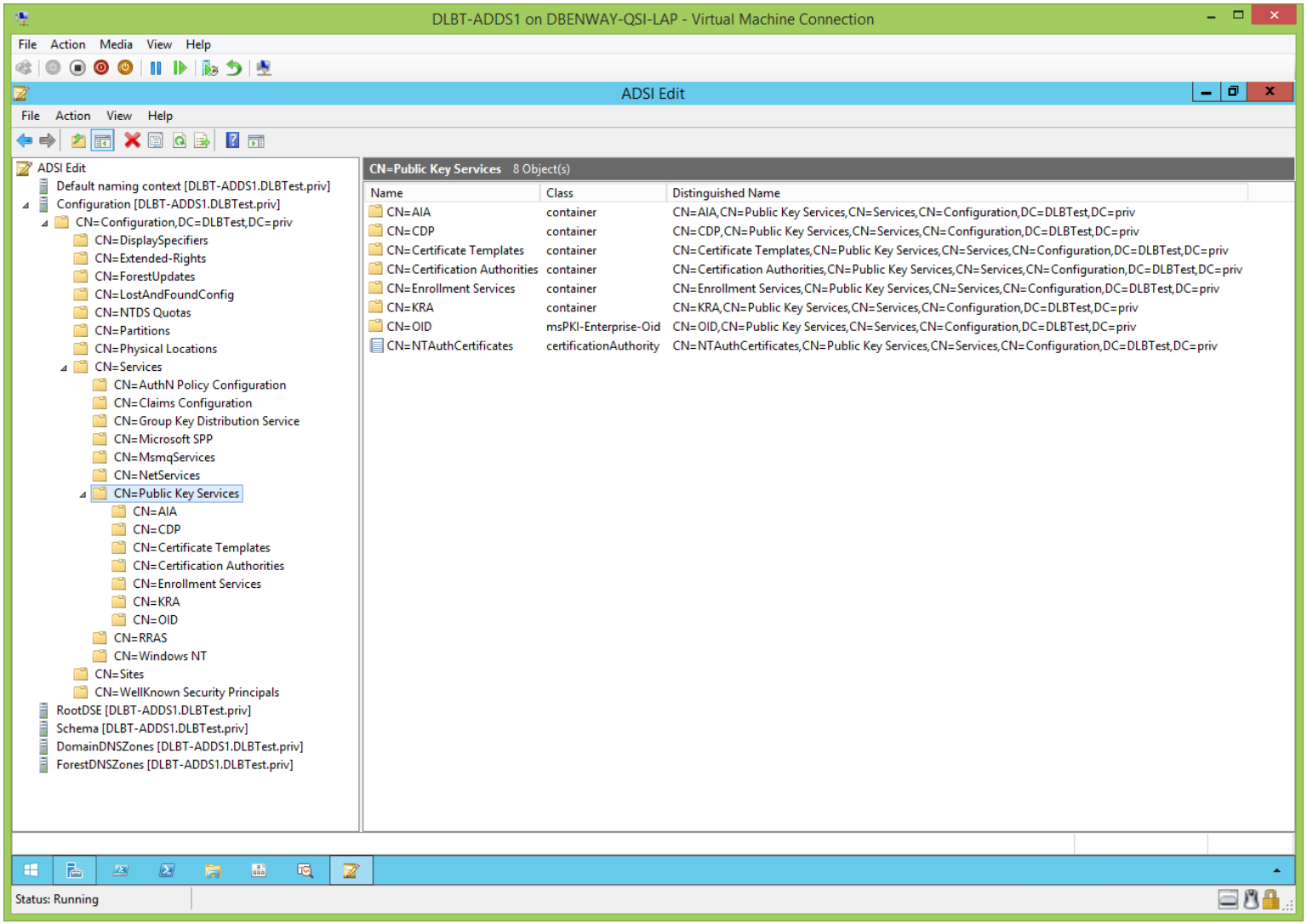
Compu Windows PowerShell ISE NE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\IntSubPolIssCA

Status: Running

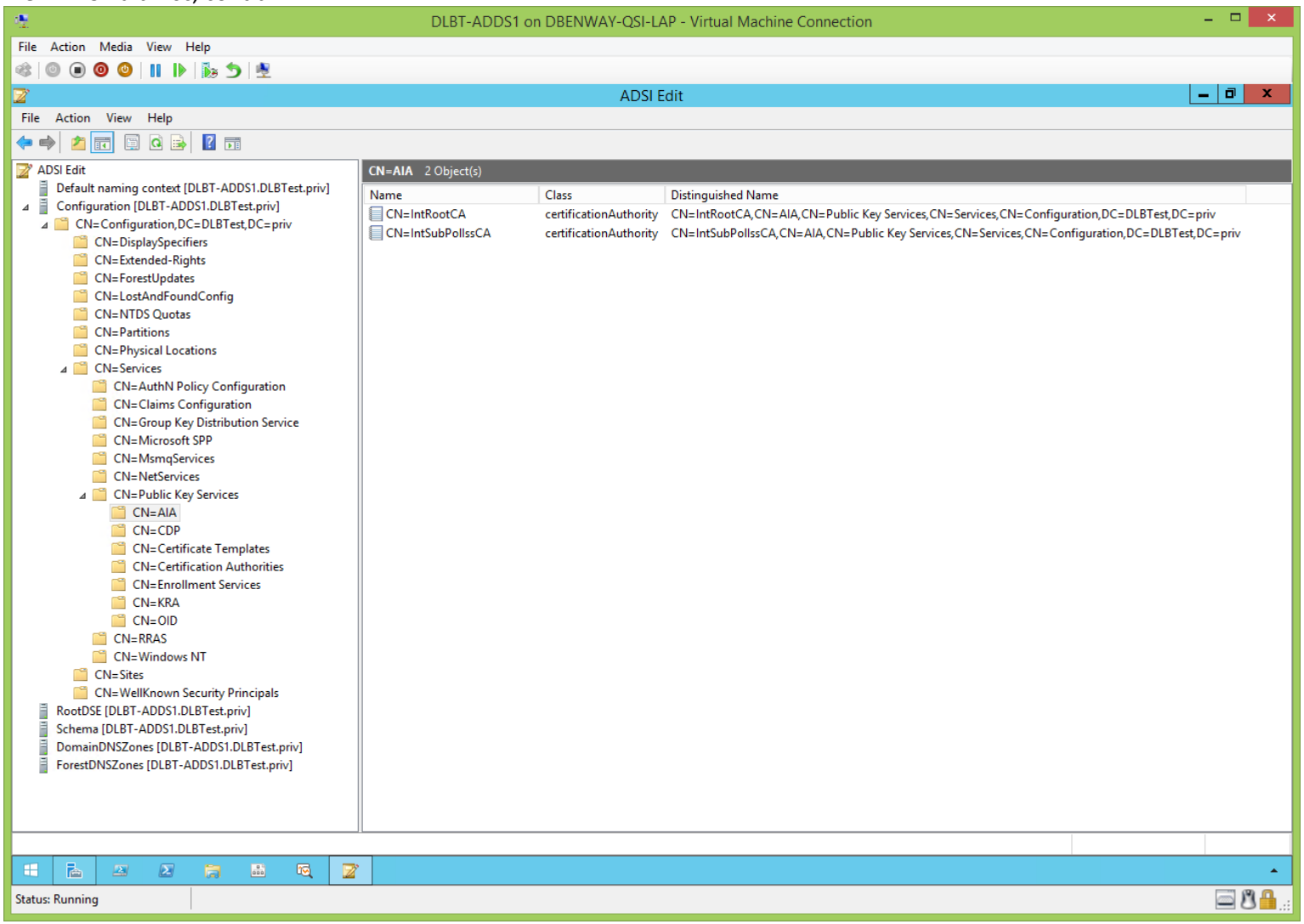
ADSIEdit.msc (After CertUtil.exe):

(jump to TOC)

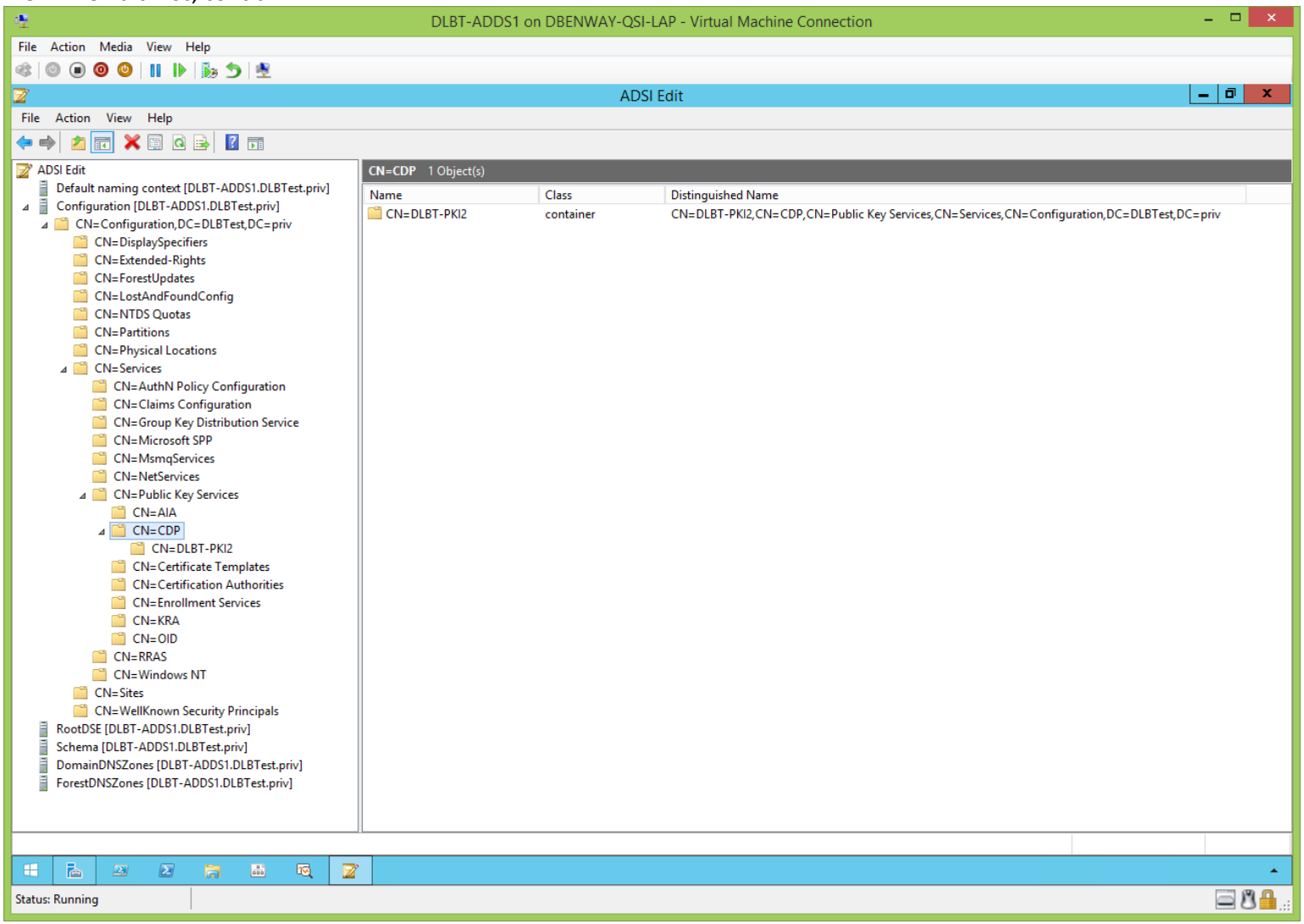
View ADSIEdit.msc:



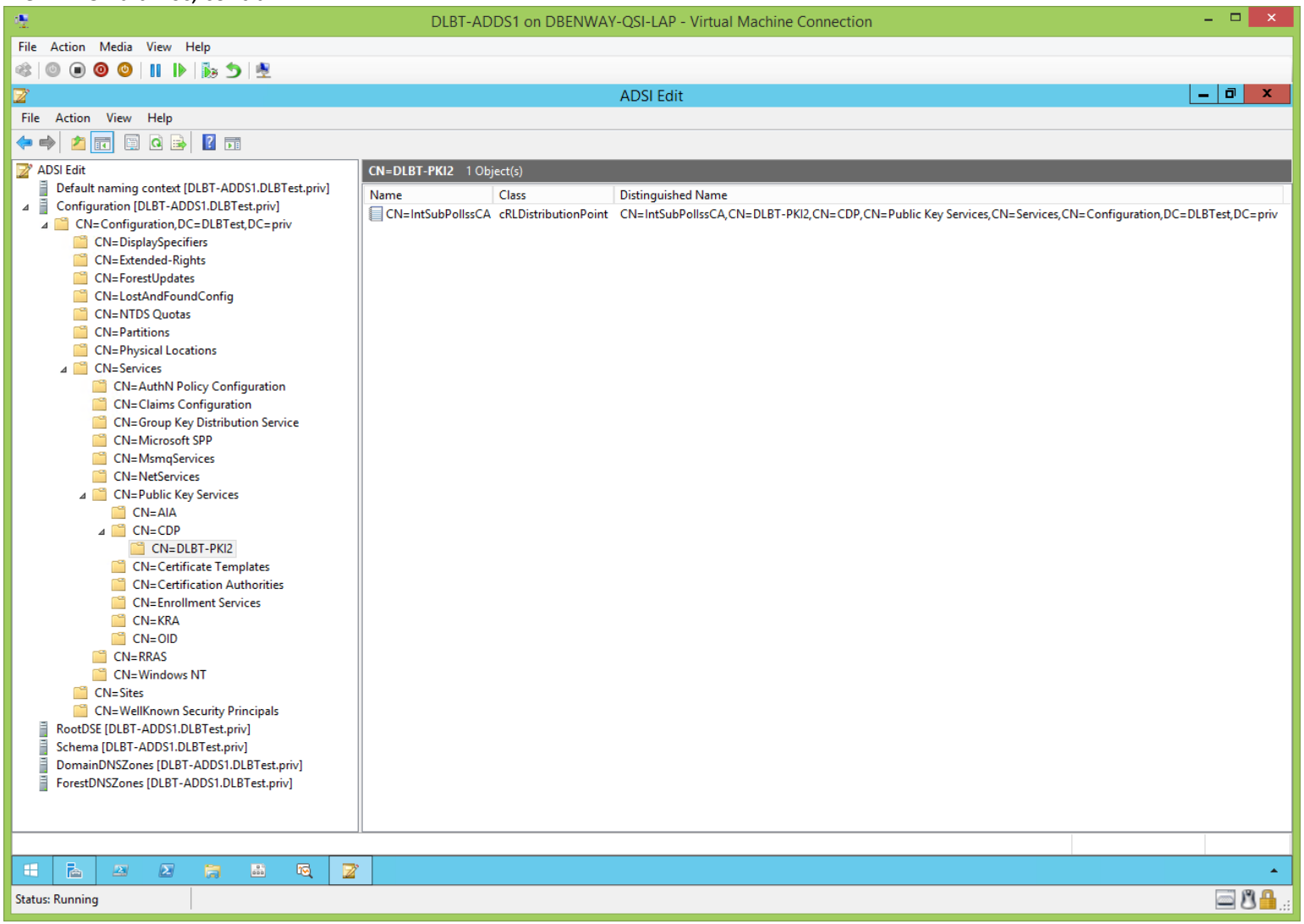
View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:

DLBT-ADDS1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

ADSI Edit

File Action View Help

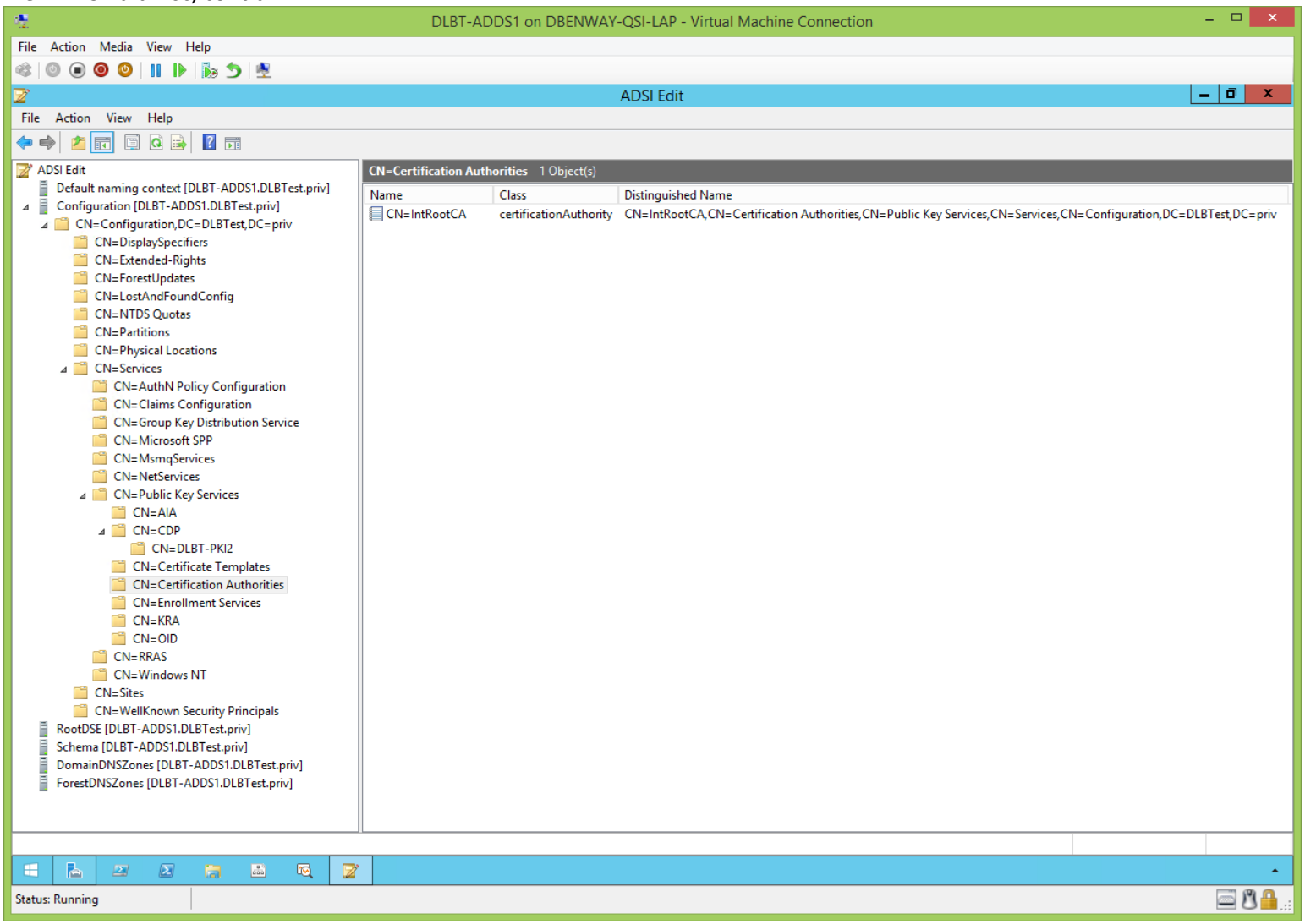
ADSI Edit
- Default naming context [DLBT-ADDS1.DLBTest.priv]
- Configuration [DLBT-ADDS1.DLBTest.priv]
  - CN=Configuration,DC=DLBTest,DC=priv
    - CN=DisplaySpecifiers
    - CN=Extended-Rights
    - CN=ForestUpdates
    - CN=LostAndFoundConfig
    - CN=NTDS Quotas
    - CN=Partitions
    - CN=Physical Locations
    - CN=Services
      - CN=AuthN Policy Configuration
      - CN=Claims Configuration
      - CN=Group Key Distribution Service
      - CN=Microsoft SPP
      - CN=MsmqServices
      - CN=NetServices
      - CN=Public Key Services
        - CN=AIA
        - CN=CDP
          - CN=DLBT-PKI2
        - CN=Certificate Templates
        - CN=Certification Authorities
        - CN=Enrollment Services
        - CN=KRA
        - CN=OID
      - CN=RRAS
      - CN=Windows NT
    - CN=Sites
    - CN=WellKnown Security Principals
- RootDSE [DLBT-ADDS1.DLBTest.priv]
- Schema [DLBT-ADDS1.DLBTest.priv]
- DomainDNSZones [DLBT-ADDS1.DLBTest.priv]
- ForestDNSZones [DLBT-ADDS1.DLBTest.priv]

CN=Certificate Templates 33 Object(s)

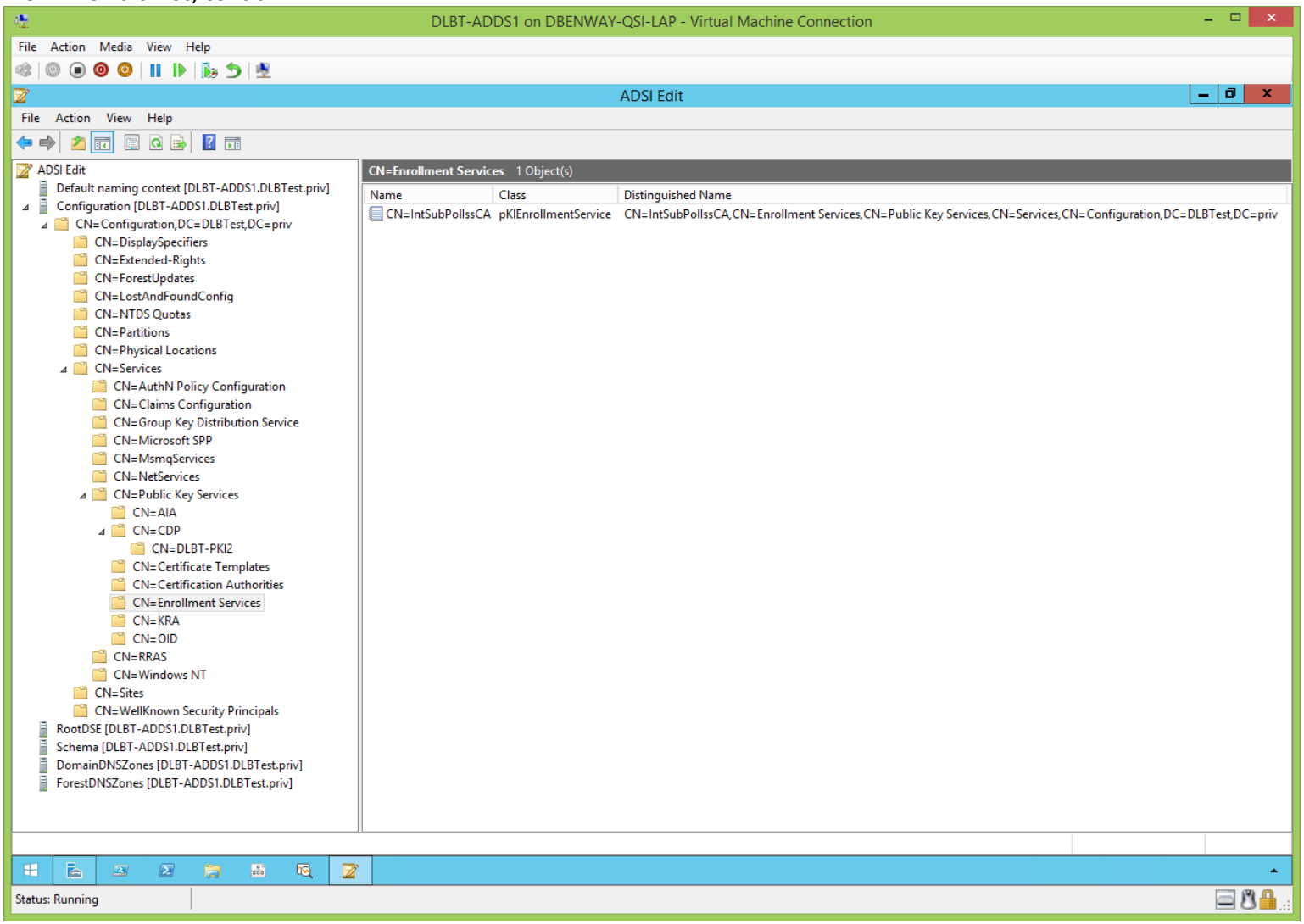
Name	Class	Distinguished Name
CN=Administrator	pKICertificateTem...	CN=Administrator,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=CA	pKICertificateTem...	CN=CA,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=CAExchange	pKICertificateTem...	CN=CAExchange,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=CEPEncryption	pKICertificateTem...	CN=CEPEncryption,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=p..
CN=ClientAuth	pKICertificateTem...	CN=ClientAuth,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=CodeSigning	pKICertificateTem...	CN=CodeSigning,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=CrossCA	pKICertificateTem...	CN=CrossCA,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=CTLSigning	pKICertificateTem...	CN=CTLSigning,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=DirectoryEma...	pKICertificateTem...	CN=DirectoryEmailReplication,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DL...
CN=DomainCont...	pKICertificateTem...	CN=DomainController,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,D...
CN=DomainCont...	pKICertificateTem...	CN=DomainControllerAuthentication,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,...
CN=EFS	pKICertificateTem...	CN=EFS,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=EFSRecovery	pKICertificateTem...	CN=EFSRecovery,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=EnrollmentA...	pKICertificateTem...	CN=EnrollmentAgent,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC...
CN=EnrollmentA...	pKICertificateTem...	CN=EnrollmentAgentOffline,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBT..
CN=ExchangeUser	pKICertificateTem...	CN=ExchangeUser,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=ExchangeUse...	pKICertificateTem...	CN=ExchangeUserSignature,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBT...
CN=IPSECInterme...	pKICertificateTem...	CN=IPSECIntermediateOffline,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLB..
CN=IPSECInterme...	pKICertificateTem...	CN=IPSECIntermediateOnline,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLB...
CN=KerberosAut...	pKICertificateTem...	CN=KerberosAuthentication,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBT...
CN=KeyRecovery...	pKICertificateTem...	CN=KeyRecoveryAgent,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,D...
CN=Machine	pKICertificateTem...	CN=Machine,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=MachineEnrollmentAgent	ateTem...	CN=MachineEnrollmentAgent,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DL...
CN=OCSPRespon...	pKICertificateTem...	CN=OCSPResponseSigning,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTe..
CN=OfflineRouter	pKICertificateTem...	CN=OfflineRouter,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=RASAndIASS...	pKICertificateTem...	CN=RASAndIASServer,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC...
CN=SmartcardLo...	pKICertificateTem...	CN=SmartcardLogon,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC...
CN=SmartcardUser	pKICertificateTem...	CN=SmartcardUser,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=p..
CN=SubCA	pKICertificateTem...	CN=SubCA,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=User	pKICertificateTem...	CN=User,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=UserSignature	pKICertificateTem...	CN=UserSignature,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv
CN=WebServer	pKICertificateTem...	CN=WebServer,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=DLBTest,DC=priv

Status: Running

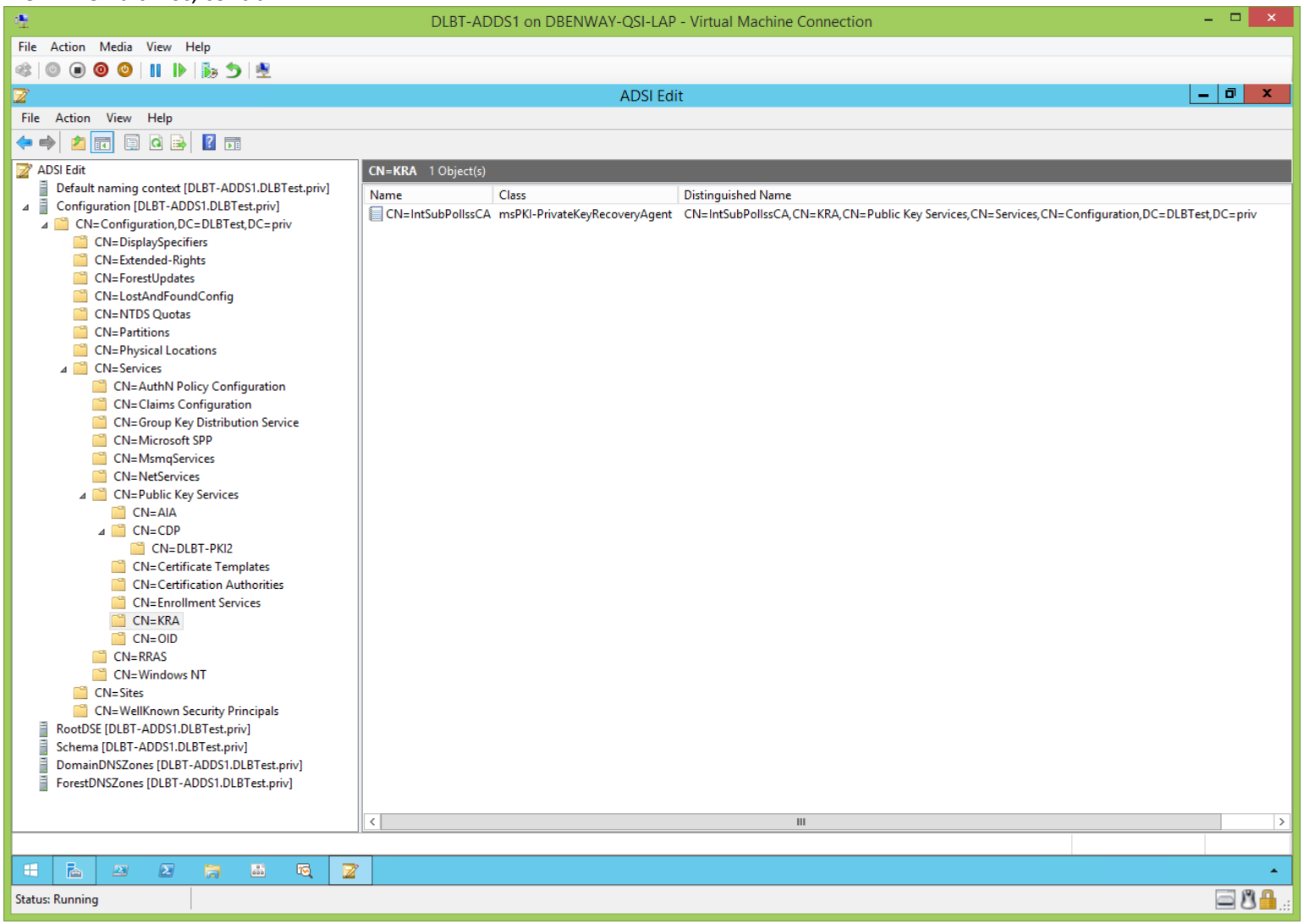
View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:



View ADSIEdit.msc, cont'd:

DLBT-ADDS1 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

ADSI Edit

File Action View Help

ADSI Edit
- Default naming context [DLBT-ADDS1.DLBTest.priv]
- Configuration [DLBT-ADDS1.DLBTest.priv]
  - CN=Configuration,DC=DLBTest,DC=priv
    - CN=DisplaySpecifiers
    - CN=Extended-Rights
    - CN=ForestUpdates
    - CN=LostAndFoundConfig
    - CN=NTDS Quotas
    - CN=Partitions
    - CN=Physical Locations
    - CN=Services
      - CN=AuthN Policy Configuration
      - CN=Claims Configuration
      - CN=Group Key Distribution Service
      - CN=Microsoft SPP
      - CN=MsmqServices
      - CN=NetServices
      - CN=Public Key Services
        - CN=AIA
        - CN=CDP
          - CN=DLBT-PKI2
        - CN=Certificate Templates
        - CN=Certification Authorities
        - CN=Enrollment Services
        - CN=KRA
        - CN=OID
      - CN=RRAS
      - CN=Windows NT
    - CN=Sites
    - CN=WellKnown Security Principals
- RootDSE [DLBT-ADDS1.DLBTest.priv]
- Schema [DLBT-ADDS1.DLBTest.priv]
- DomainDNSZones [DLBT-ADDS1.DLBTest.priv]
- ForestDNSZones [DLBT-ADDS1.DLBTest.priv]

CN=OID 12 Object(s)

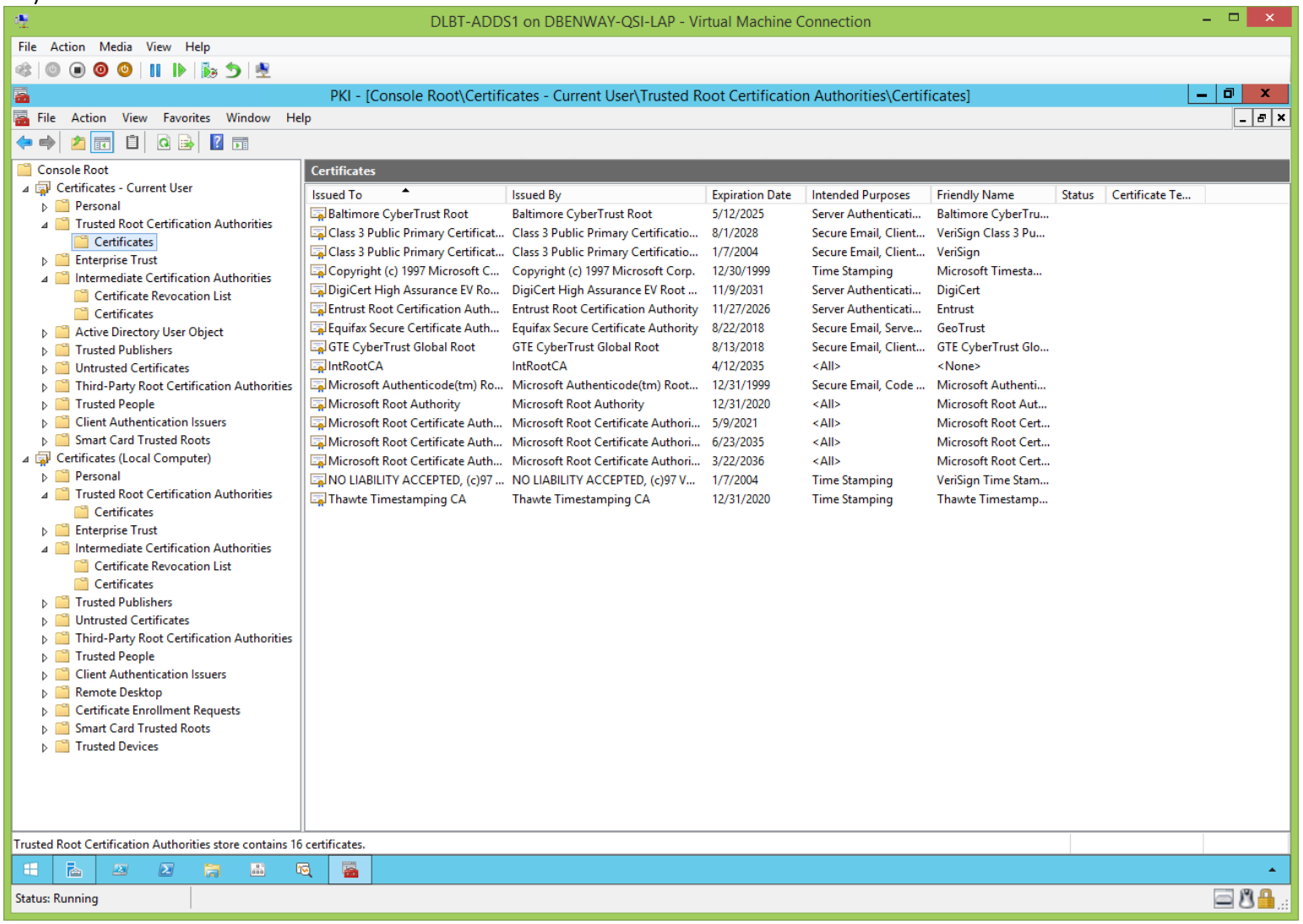
Name	Class	Distinguished Name
CN=25.0AAA4817434B4C224D71EF2E2069A658	msPKI-Enterprise-Oid	CN=25.0AAA4817434B4C224D71EF2E2069A658,CN=OID,CN=Public Key Services,CN=Services,CN=
CN=26.5ABA86A617B1FD47E3FBB12D78D20722	msPKI-Enterprise-Oid	CN=26.5ABA86A617B1FD47E3FBB12D78D20722,CN=OID,CN=Public Key Services,CN=Services,CN
CN=27.5C95A50086AAB3AA432E73DA3A48A9A7	msPKI-Enterprise-Oid	CN=27.5C95A50086AAB3AA432E73DA3A48A9A7,CN=OID,CN=Public Key Services,CN=Services,CI
CN=28.115972A1DB64D144BE190BE88AA48A37	msPKI-Enterprise-Oid	CN=28.115972A1DB64D144BE190BE88AA48A37,CN=OID,CN=Public Key Services,CN=Services,CN:
CN=29.51CE5C9C23AE82502C78FA5384B5AD60	msPKI-Enterprise-Oid	CN=29.51CE5C9C23AE82502C78FA5384B5AD60,CN=OID,CN=Public Key Services,CN=Services,CN
CN=30.7FFD00AB0DFA95CD063161ED3DE174E4	msPKI-Enterprise-Oid	CN=30.7FFD00AB0DFA95CD063161ED3DE174E4,CN=OID,CN=Public Key Services,CN=Services,CN
CN=31.42FBA1500E6B67BEF8D90B38B5D914F3	msPKI-Enterprise-Oid	CN=31.42FBA1500E6B67BEF8D90B38B5D914F3,CN=OID,CN=Public Key Services,CN=Services,CN=
CN=32.41F15524E605111A781E47C6F2734692	msPKI-Enterprise-Oid	CN=32.41F15524E605111A781E47C6F2734692,CN=OID,CN=Public Key Services,CN=Services,CN=C
CN=33.2C857A94D04ACCD3B3386446DF98E541	msPKI-Enterprise-Oid	CN=33.2C857A94D04ACCD3B3386446DF98E541,CN=OID,CN=Public Key Services,CN=Services,CN
CN=400.BBF51C5172B15E8111B75A81908AF1F6	msPKI-Enterprise-Oid	CN=400.BBF51C5172B15E8111B75A81908AF1F6,CN=OID,CN=Public Key Services,CN=Services,CN
CN=401.E68F75EF22F3874F804F25C890ABFFD5	msPKI-Enterprise-Oid	CN=401.E68F75EF22F3874F804F25C890ABFFD5,CN=OID,CN=Public Key Services,CN=Services,CN=
CN=402.1C836A2B5723F4DB1B8D6754F39E79E3	msPKI-Enterprise-Oid	CN=402.1C836A2B5723F4DB1B8D6754F39E79E3,CN=OID,CN=Public Key Services,CN=Services,CN

Status: Running

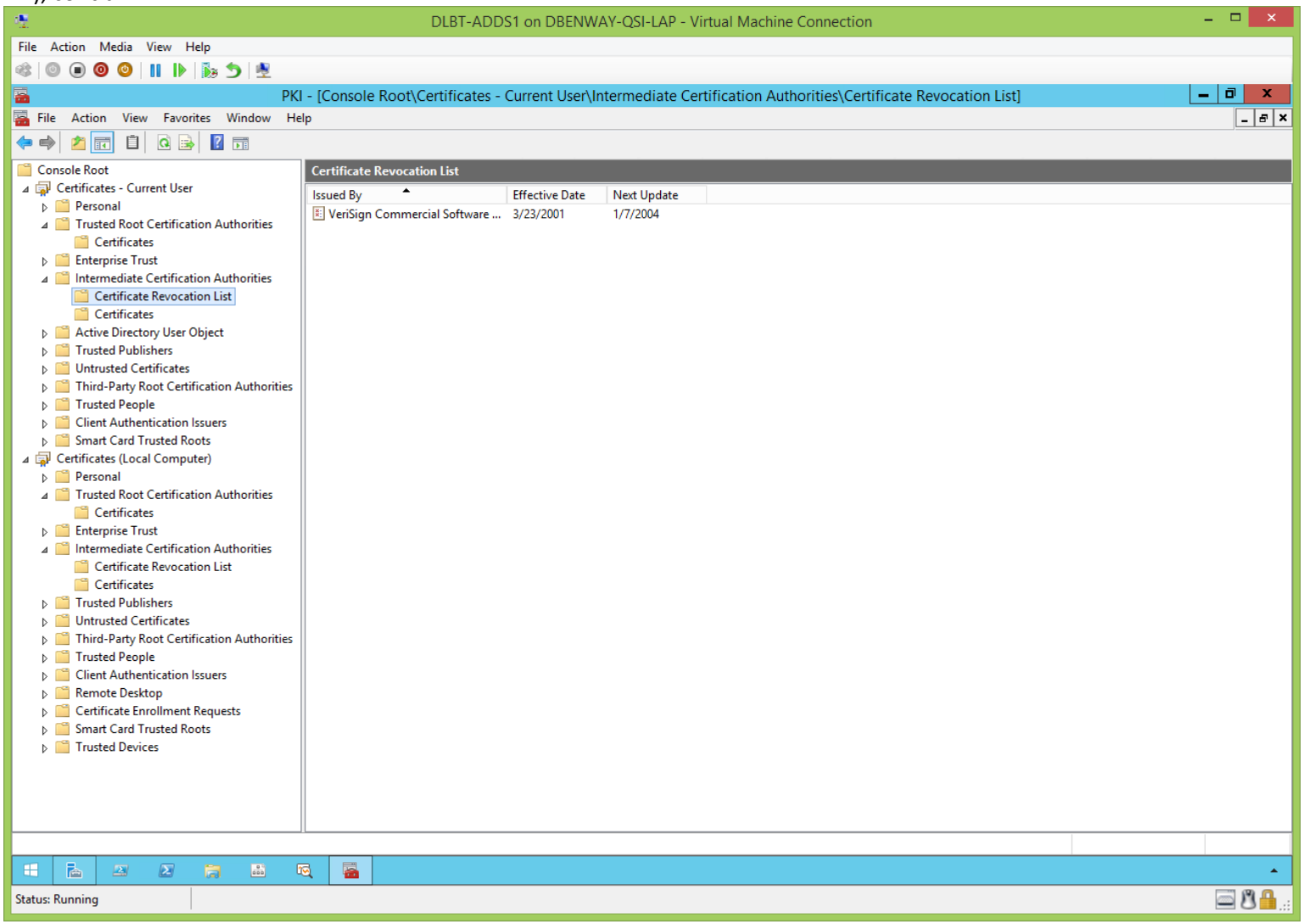
DC's Local Certificate Store (After CertUtil.exe):

(jump to TOC)

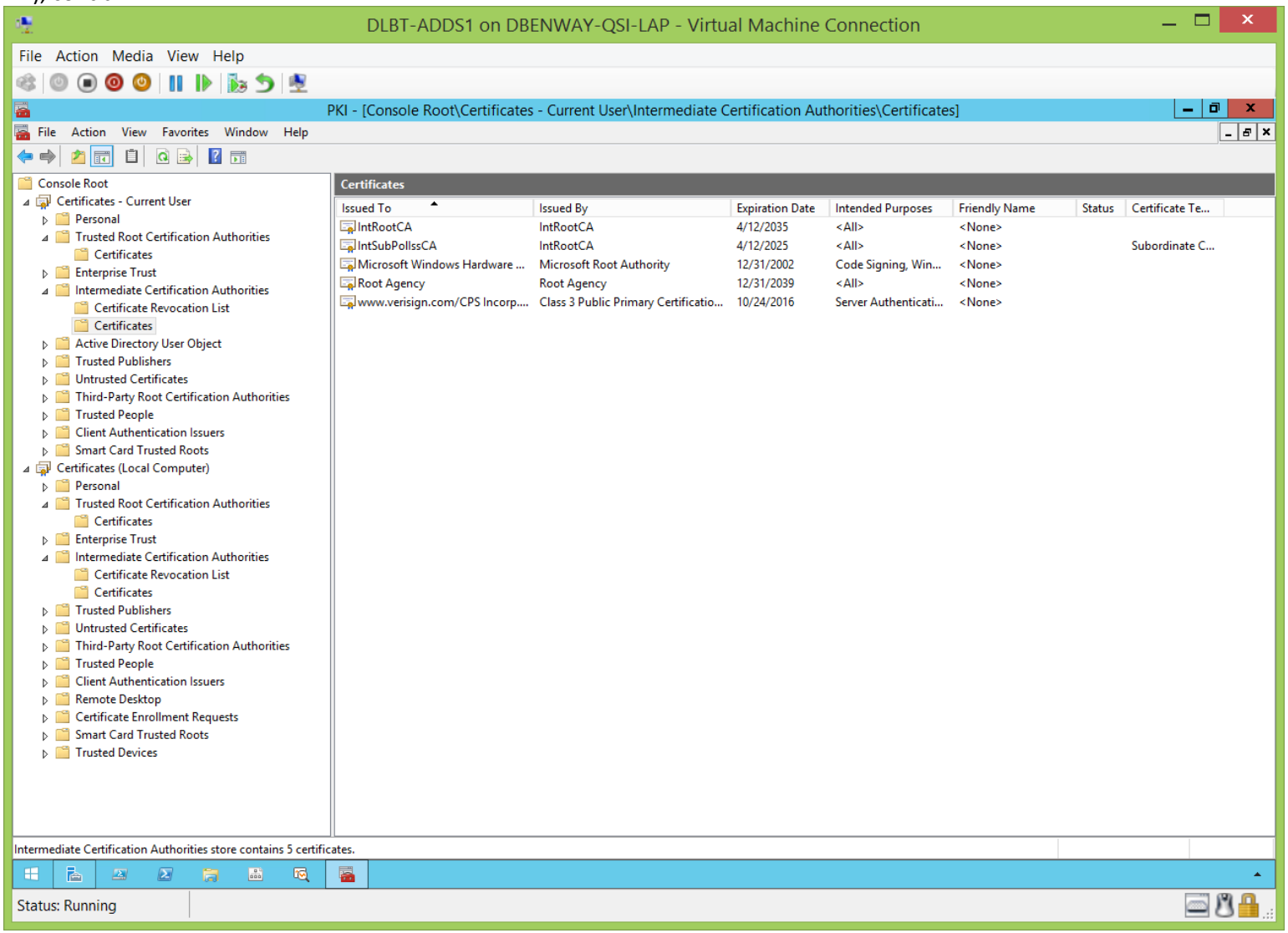
View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD):



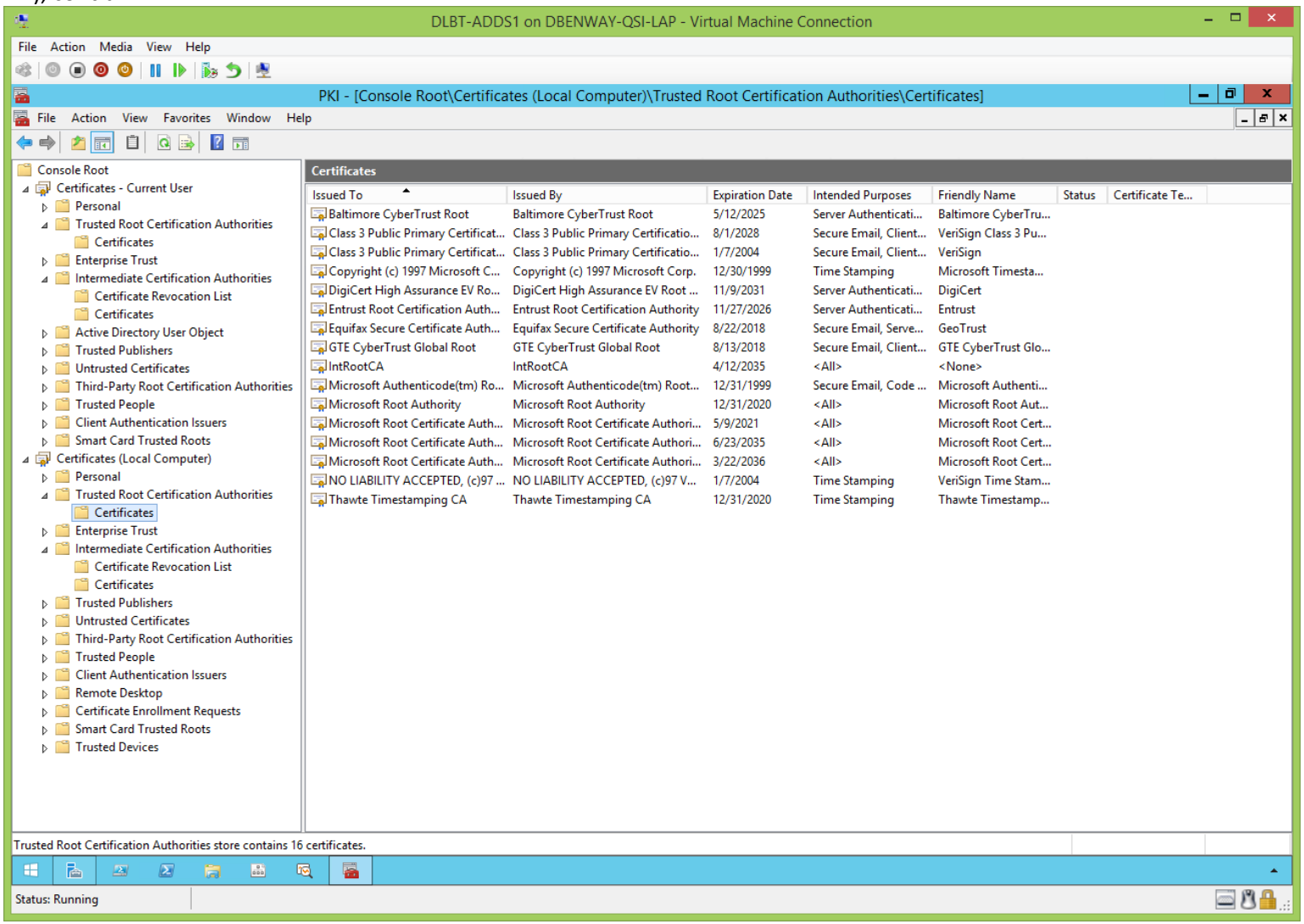
View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



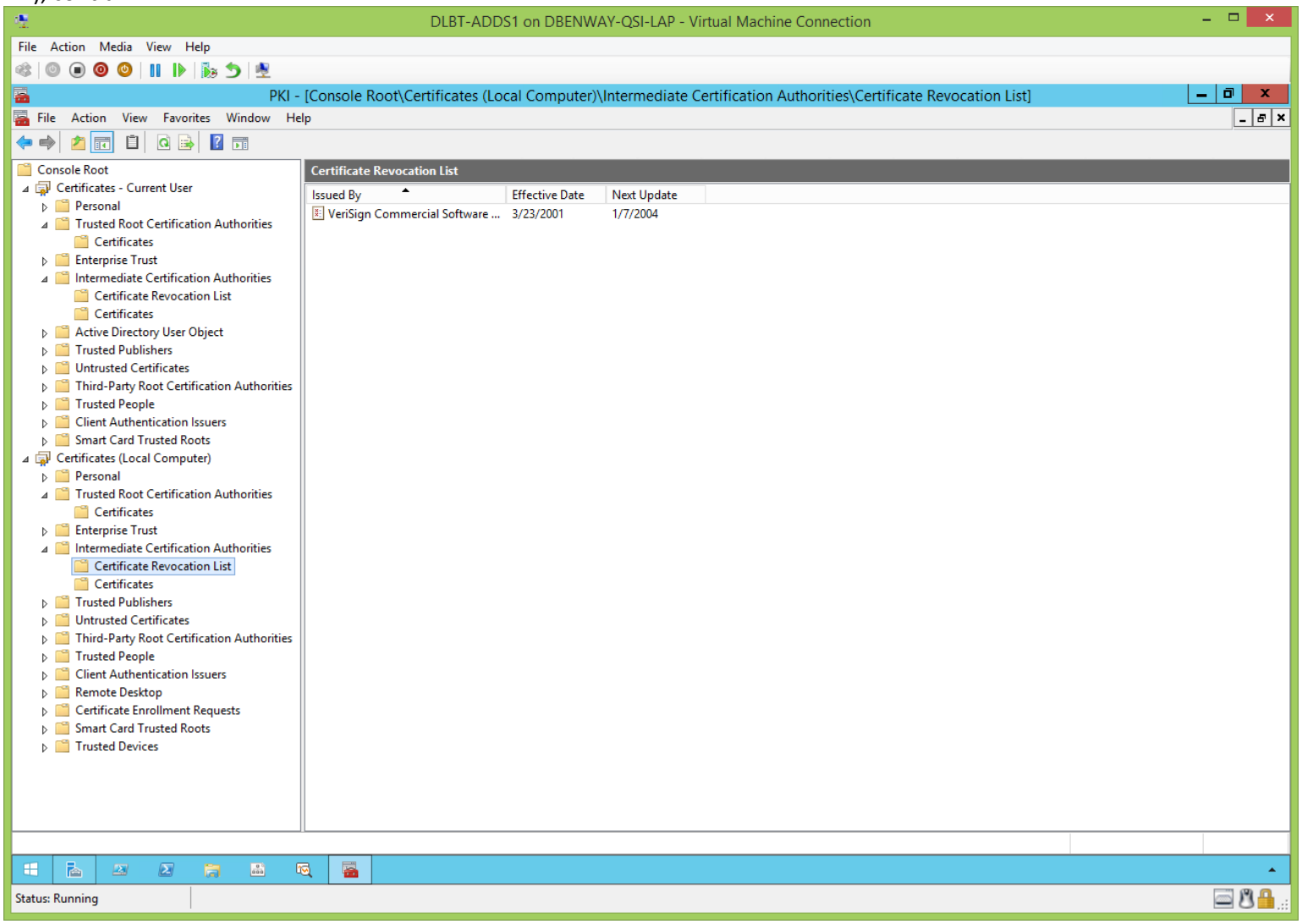
View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



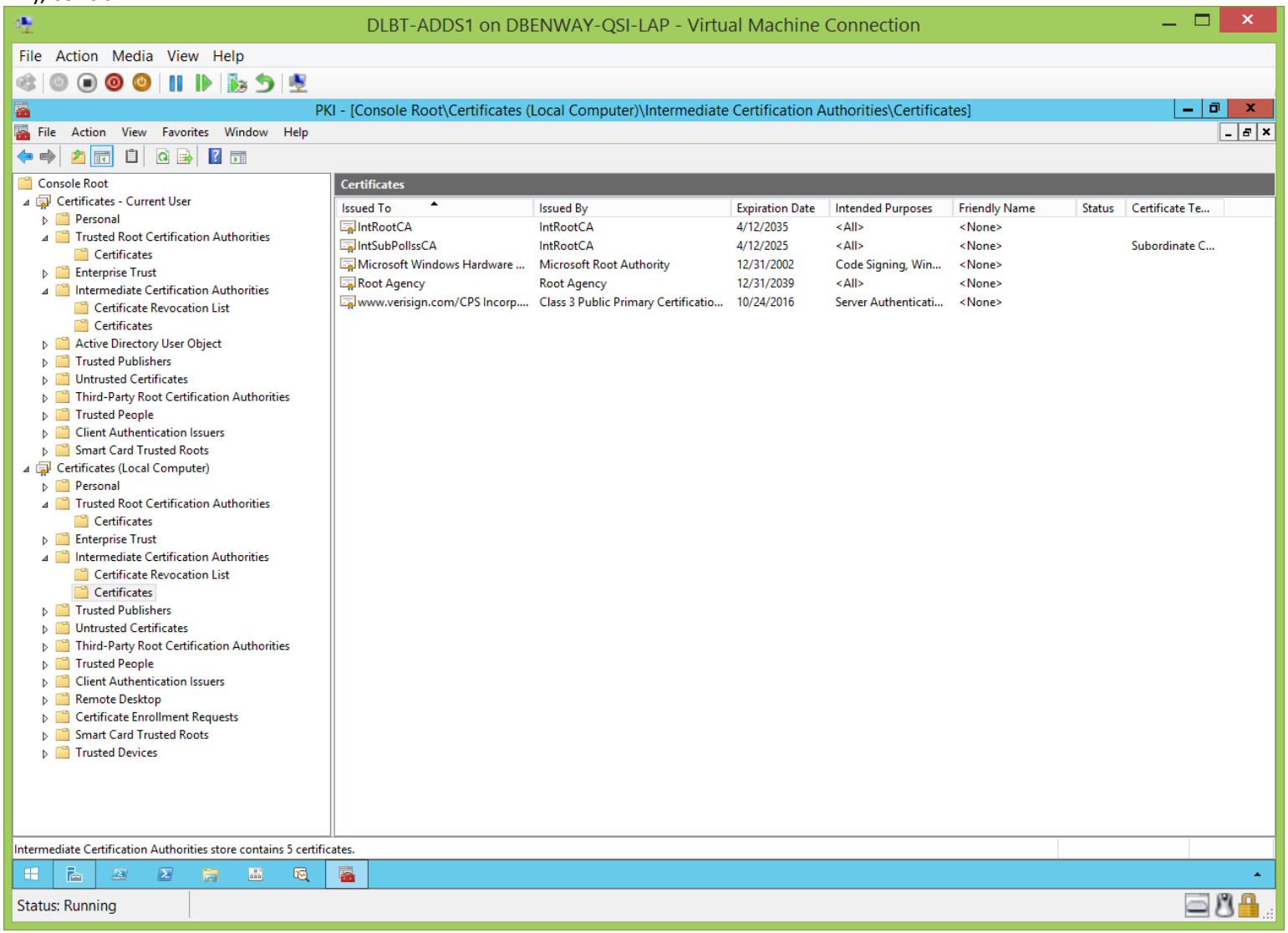
View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



View the DC's local certificate store (you might need to reboot the DC once or twice to speed up its installation of the sub/policy/issuing CA's certificate from AD), cont'd:



Sub/Policy/Issuing CA's Local Certificate Store (After CertUtil.exe):

(jump to TOC)

View sub/policy/issuing CA's local certificate store:

DLBT-PKI2 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

PKI - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificate Templates
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Smart Card Trusted Roots
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Remote Desktop
    - Smart Card Trusted Roots
    - Trusted Devices
    - Web Hosting
  - Certification Authority (Local)
  - Enterprise PKI

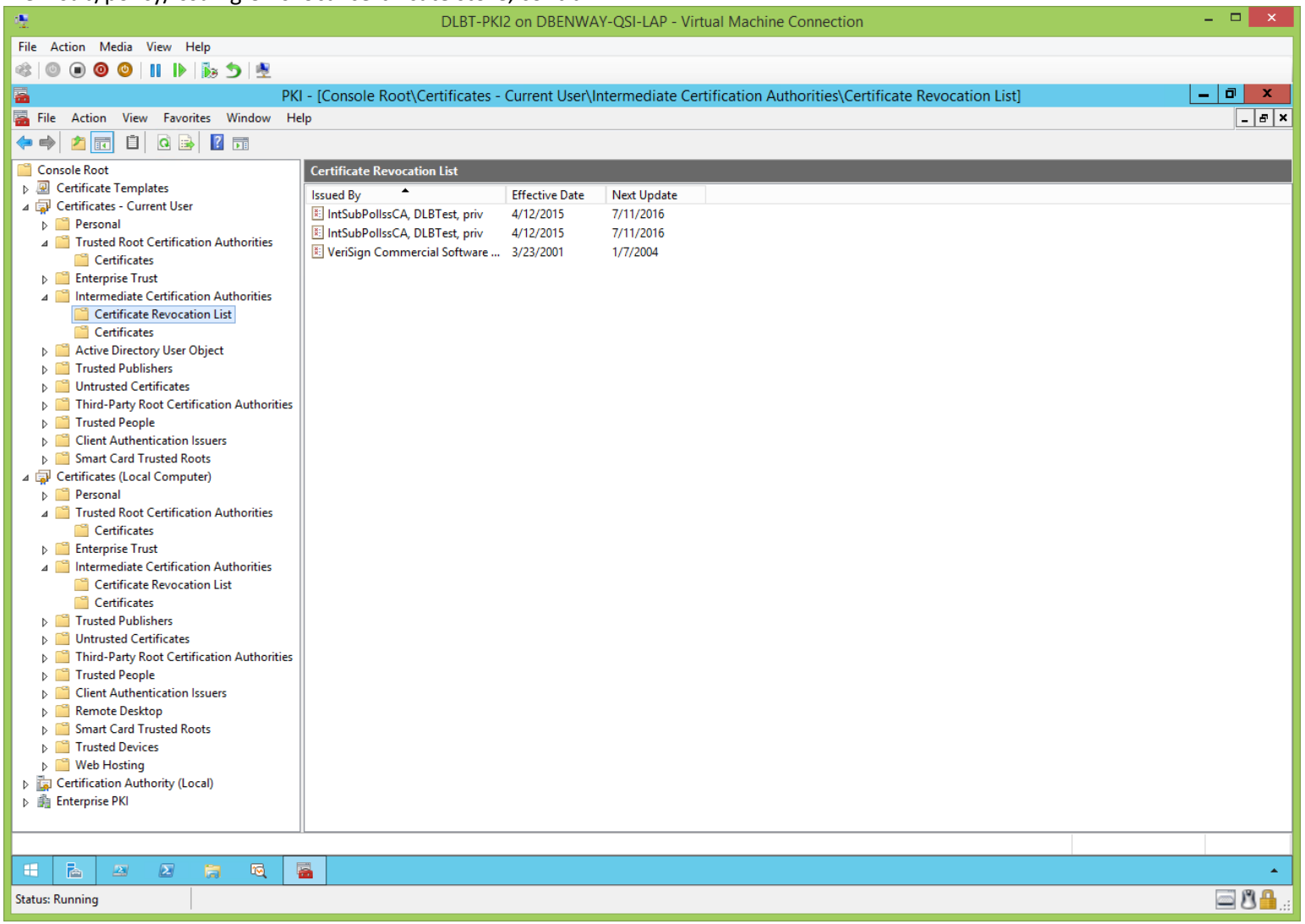
Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Server Authenticati...	Baltimore CyberTru...		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...		
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
IntRootCA	IntRootCA	4/12/2035	<All>	<None>		
IntRootCA	IntRootCA	4/12/2035	<All>	<None>		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...		
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...		

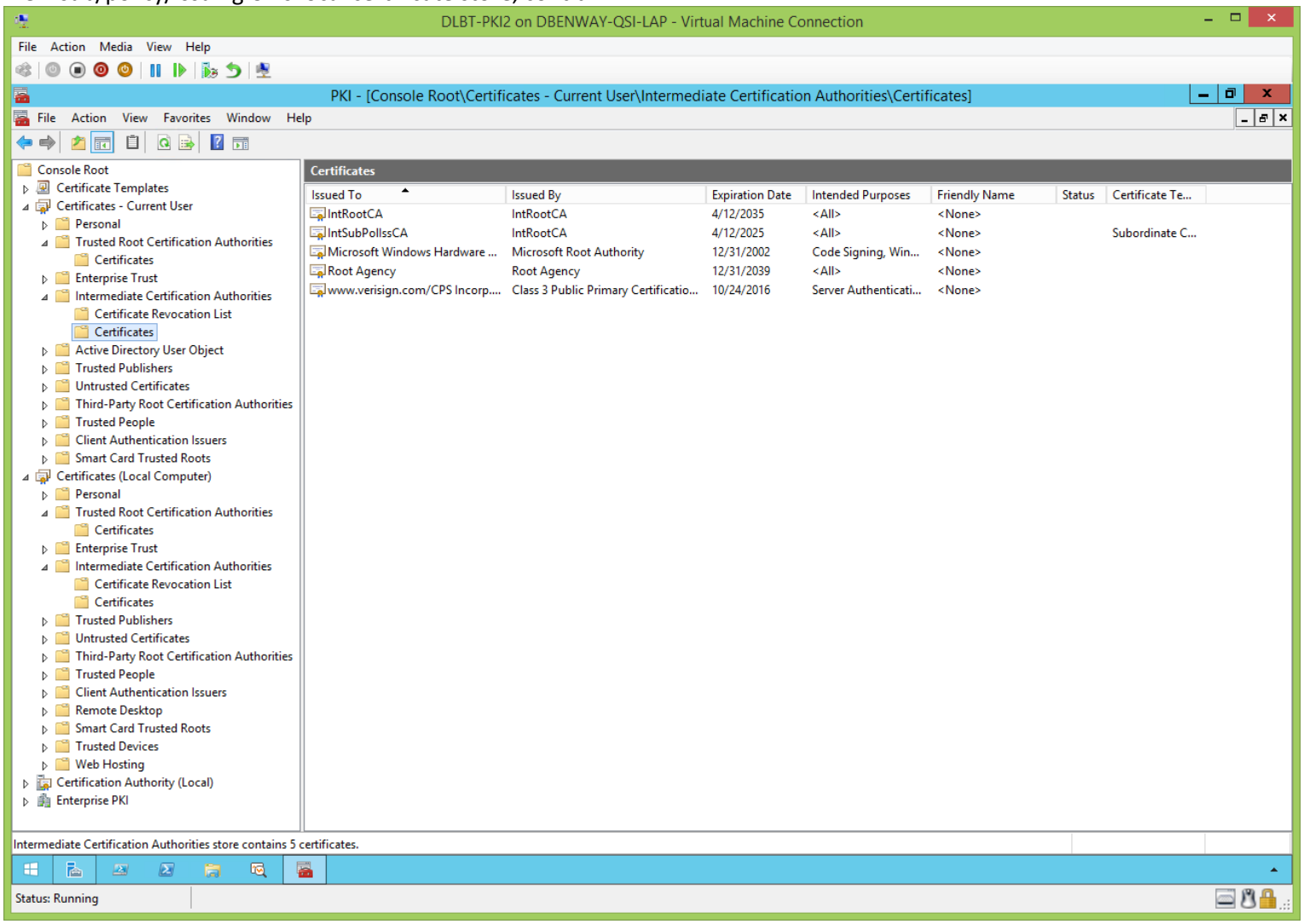
Trusted Root Certification Authorities store contains 13 certificates.

Status: Running

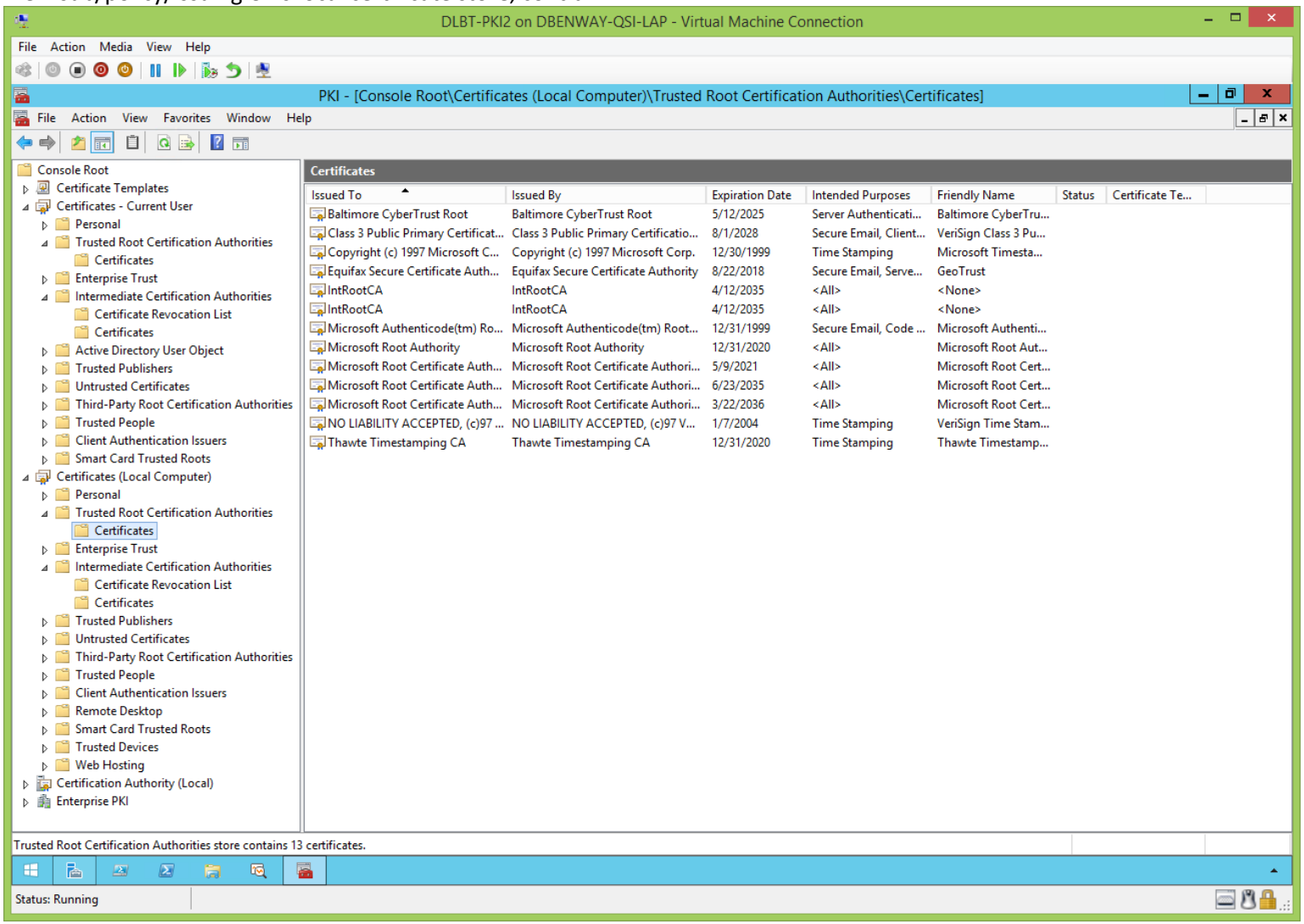
View sub/policy/issuing CA's local certificate store, cont'd:



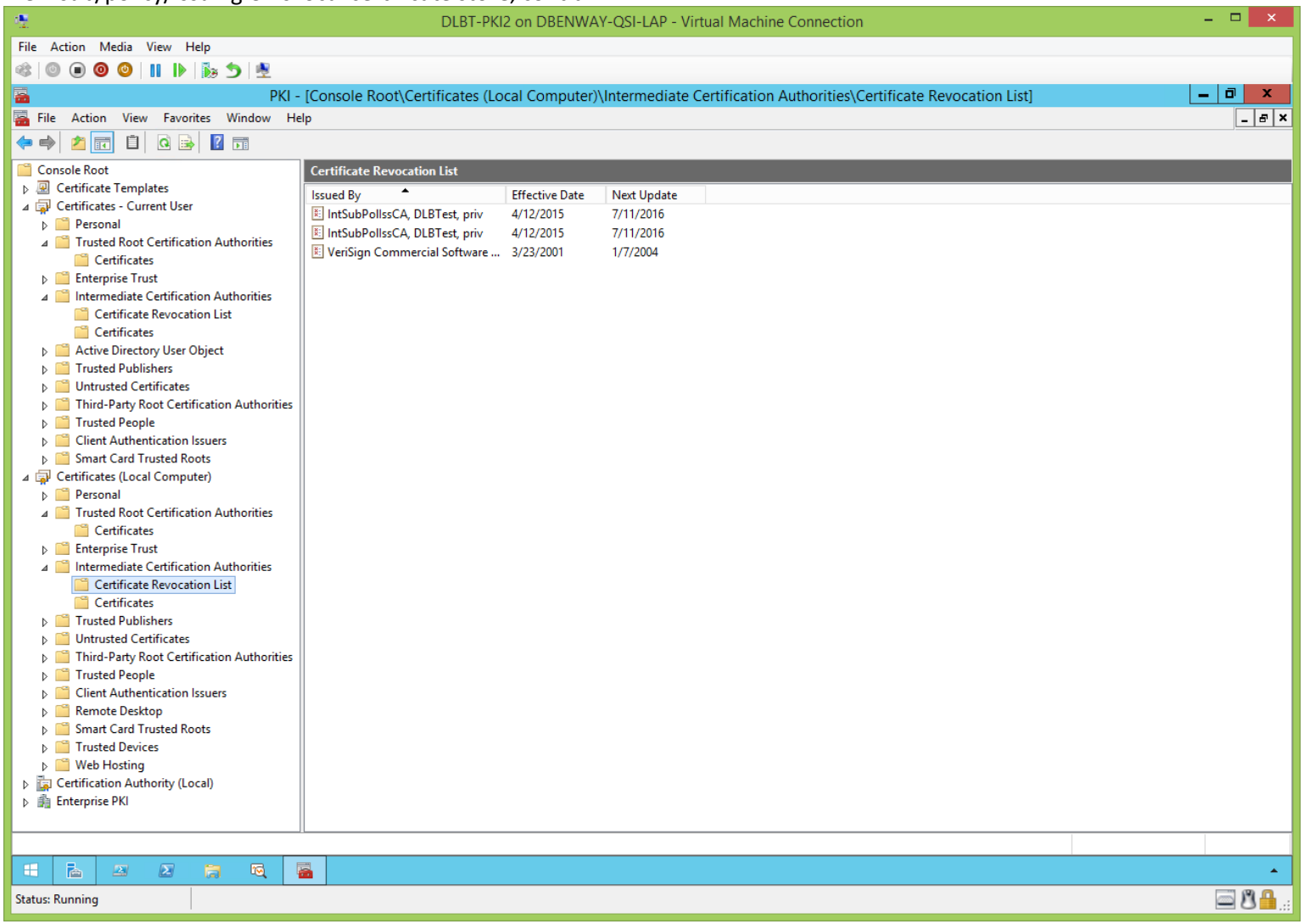
View sub/policy/issuing CA's local certificate store, cont'd:



View sub/policy/issuing CA's local certificate store, cont'd:



View sub/policy/issuing CA's local certificate store, cont'd:



View sub/policy/issuing CA's local certificate store, cont'd:

DLBT-PKI2 on DBENWAY-QSI-LAP - Virtual Machine Connection

File Action Media View Help

PKI - [Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates]

File Action View Favorites Window Help

- Console Root
  - Certificate Templates
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Smart Card Trusted Roots
  - Certificates (Local Computer)
    - Personal
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Remote Desktop
    - Smart Card Trusted Roots
    - Trusted Devices
    - Web Hosting
  - Certification Authority (Local)
  - Enterprise PKI

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
IntRootCA	IntRootCA	4/12/2035	<All>	<None>		
IntSubPolIssCA	IntRootCA	4/12/2025	<All>	<None>		Subordinate C...
Microsoft Windows Hardware ...	Microsoft Root Authority	12/31/2002	Code Signing, Win...	<None>		
Root Agency	Root Agency	12/31/2039	<All>	<None>		
www.verisign.com/CPS Incorp....	Class 3 Public Primary Certificatio...	10/24/2016	Server Authenticati...	<None>		

Intermediate Certification Authorities store contains 5 certificates.

Status: Running

Exit Module:

(jump to TOC)

It is beyond the scope of this lab document to show the setup of the SMTP Exit Module. However, it should be researched and almost certainly deployed in any production environment because of its major benefits with respect to CA recovery. For more information do an Internet search on "SMTP Exit Module CA Recovery". Following is a particularly good article:

Operating a PKI: SMTP Exit Module: https://blogs.technet.microsoft.com/xdot509/2013/06/17/operating-a-pki-smtp-exit-module/

KRA (Key Recovery Agent):

(jump to TOC)

https://technet.microsoft.com/en-us/library/Cc730721.aspx
Managing Key Archival and Recovery

> Key archival and recovery are not enabled by default. This is because many organizations would consider the storage of the private key in multiple locations to be a security vulnerability. Requiring organizations to make explicit decisions about which certificates are covered by key archival and recovery and who can recover archived keys helps ensure that key archival and recovery are used to enhance security rather than detract from security.
>
> When users lose their private keys, any information that was persistently encrypted with the corresponding public key is no longer accessible. Using key archival and recovery helps protect encrypted data from permanent loss if, for example, an operating system needs to be reinstalled, the user account to which the encryption key was originally issued is no longer available, or the key is otherwise no longer accessible. To help protect private keys, Microsoft enterprise certification authorities (CAs) can archive a user's keys in its database when certificates are issued. These keys are encrypted and stored by the CA.
>
> This private key archive makes it possible for the key to be recovered at a later time. The key recovery process requires an administrator to retrieve the encrypted certificate and private key and then a key recovery agent to decrypt them. When a correctly signed key recovery request is received, the user's certificate and private key are provided to the requester. The requester would then use the key as appropriate or securely transfer the key to the user for continued use. As long as the private key is not compromised, the certificate does not have to be replaced or renewed with a different key.

http://blogs.technet.com/b/yungchou/archive/2013/10/22/enterprise-pki-with-windows-server-2012-r2-active-directory-certificate-services-part-2-of-2.aspx
Enterprise PKI with Windows Server 2012 R2 Active Directory Certificate Services (Part 2 of 2)

DRA (Data Recovery Agent):

(jump to TOC)

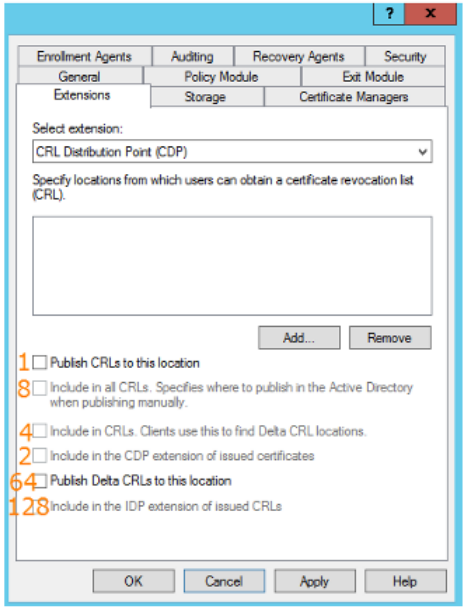
If you're using EFS or BitLocker, you should probably set up a Data Recovery Agent.

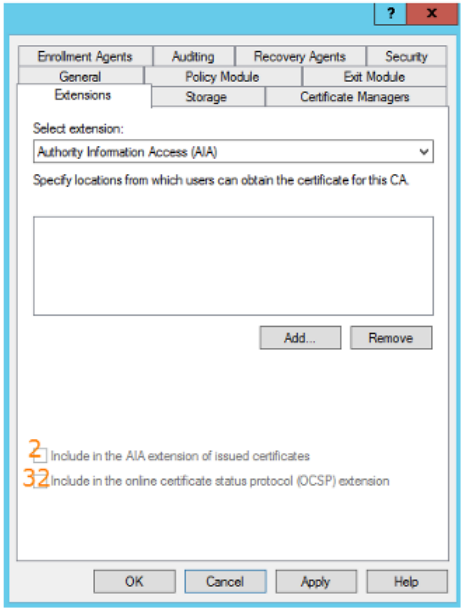
Appendix A - Extension Syntax in CertUtil.exe Files:

(jump to TOC)

For a 2-Tier, Offline-Root, Internal PKI with an IIS CDP on the sub/policy/issuing CA, I recommend these settings for certUtil.exe file values:

Root CA	CDP	local file	**65:%windir%\system32\CertSrv\CertEnroll\%3%8%9.crl** 65 = 64 + 1, which is: 64: Publish Delta CRLs to this location 1: Publish CRLs to this location
		LDAP	-
		HTTP	**134:http://PKI.DLBTest.priv/CDP/%3%8%9.crl** 134 = 128 + 4 + 2, which is: 128: Include in the IDP extension of issued CRLs 4: Include in CRLS. Clients use this to find Delta CRL locations. 2: Include in the CDP extension of issued certificates
		share	-
	AIA	local file	**0:%windir%\system32\CertSrv\CertEnroll\%1_%3%4.crt** 0 is: no checkboxes
		LDAP	-
		HTTP	**2:http://PKI.DLBTest.priv/AIA/%1_%3%4.crt** 2 is: Include in the AIA extension of issued certificates
		share	-
Sub/Issue CA	CDP	local file	**65:%windir%\system32\CertSrv\CertEnroll\%3%8%9.crl** 65 = 64 + 1, which is: 64: Publish Delta CRLs to this location 1: Publish CRLs to this location
		local file	**65:C:\InetPub\PKI\CDP\%3%8%9.crl** 65 = 64 + 1, which is: 64: Publish Delta CRLs to this location 1: Publish CRLs to this location
		LDAP	-
		HTTP	**134:http://PKI.DLBTest.priv/CDP/%3%8%9.crl** 134 = 128 + 4 + 2, which is: 128: Include in the IDP extension of issued CRLs 4: Include in CRLS. Clients use this to find Delta CRL locations. 2: Include in the CDP extension of issued certificates
		share	-
	AIA	local file	**0:%windir%\system32\CertSrv\CertEnroll\%1_%3%4.crt** 0 is: no checkboxes
		local file	**0:C:\InetPub\PKI\AIA\%1_%3%4.crt** 0 is: no checkboxes
		LDAP	-
		HTTP	**2:http://PKI.DLBTest.priv/AIA/%1_%3%4.crt** 2 is: Include in the AIA extension of issued certificates
		share	-





Appendix B - %1_ Removal from AIA Extensions:

(jump to TOC)

---
https://social.technet.microsoft.com/Forums/windowsserver/en-US/15f265bc-1ef1-42af-a568-c9115e53ccf7/how-to-configure-aia-without-serverdnsname-also-known-as-1-in-registry-or-1-in-a-postscript?forum=winserversecurity
How to configure AIA without <ServerDNSName> also known as %1 in Registry or %%1 in a Postscript...

---
http://kazmierczak.eu/itblog/2012/08/22/the-dos-and-donts-of-pki-microsoft-adcs
The DOs and DON'Ts of PKI – Microsoft ADCS

To Remove the %1_ from AIA Extensions:

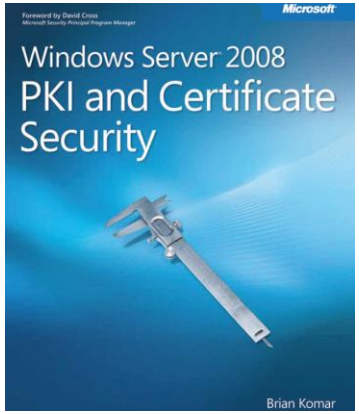
1. create the root CA, and run the CertUtil.exe commands (with no %1_ in AIA)
2. before publishing the root CA's certificate to AD or the CDP, edit its filename in C:\Windows\System32\CertSrv\CertEnroll to no longer include the root CA's FQDN
3. publish the root CA's certificate to AD and the CDP
   ---
4. create the sub/policy/issuing CA, and run the CertUtil.exe commands (with no %1_ in AIA)
5. before publishing the sub/policy/issuing CA's certificate to the CDP, edit its filename in C:\Windows\System32\CertSrv\CertEnroll to no longer include the sub/policy/issuing CA's FQDN
6. publish the sub/policy/issuing CA's certificate to the CDP

When renewing either CA's certificate, follow a similar procedure.

Bibliography:

(jump to TOC)

- Brian Komar, Windows Server 2008 PKI and Certificate Security (hard to find in print, easy to download as an eBook from Microsoft Press Store)



- CHDelay, Christopher Delay, Premier Field Engineer with Microsoft
  - http://blogs.technet.com/b/xdot509
  - https://www.youtube.com/watch?v=Q-1Y1ZI9R6k
    Root CA Renewal
  - https://www.youtube.com/watch?v=7t9ZgD_xuaA
    Issuing CA Certificate Renewal
  - http://blogs.technet.com/b/xdot509/archive/2012/11/26/pki-design-considerations-certificate-revocation-and-crl-publishing-strategies.aspx
    PKI Design Considerations: Certificate Revocation and CRL Publishing Strategies

- Andrzej Kaźmierczak
  - http://kazmierczak.eu/itblog/2012/08/22/the-dos-and-donts-of-pki-microsoft-adcs